Cybersecurity in the energy sector: what does it mean for network regulation?

July 2018

CAMBRIDGE ECONOMIC POLICY ASSOCIATES

Queens House, 55-56 Lincoln's Inn Fields
London WC2A 3LJ

Tel: 020 7269 0210
info@cepa.co.uk
www.cepa.co.uk

CEPA Ltd
@CepaLtd

Introduction

Security of supply and network resilience are of broad and current interest at the moment, especially in the utilities sphere. Security of supply tends to have a prominent role in most price control reviews for network and infrastructure companies in the UK and abroad.

Historically, focus has been on certain aspects of security of supply such as the system's ability to respond to sudden changes in the supply-demand balance, and the availability of sufficient capacity in the longer-term[1]. However, cyber threats to security are becoming increasingly prominent, as they can have important ramifications on both the short-term and the long-term.

In the first RIIO price control (RIIO-1) review, cybersecurity, known as "enhanced security costs (IT systems)" by Ofgem, was not a prominent topic due to the uncertainty around such costs and the fact that network companies had not requested specific allowances. Instead, Ofgem decided to consider these costs under an uncertainty mechanism with two possible re-openers during the eight-year price control. A re-opener mechanism was included in the price controls to provide network companies the opportunity to propose adjustments to baseline expenditure for cost categories that were difficult to accurately anticipate at the time of setting allowances. Ofgem specified two reopener windows: May 2015 and May 2018.

Ofgem's 2nd re-opener closed on 20 June 2018 and it is currently reviewing submissions, including a joint submission from National Grid Electricity Transmission and National Grid Gas Transmission about enhanced security plans. Ofgem is expected to publish its decision in September 2018.

Ahead of RIIO-2, Ofgem may choose to consider the regulatory approach for cyber costs. Additionally, companies may decide to enhance the interaction between their regulatory economists and cybersecurity engineers to develop well-justified requests for cyber cost allowances to be included in their business plans.

This briefing note explains the importance of cybersecurity in the energy sector and how it is likely to have a more prominent role in the RIIO-2 price control review[2].

[1] International Energy Agency. Energy security.

[2] Note that cyber threats are also relevant to the water and aviation sectors as recently highlighted by Ofwat and the Civil Aviation Authority (CAA). Both regulators set out expectations that regulated companies' business plans would demonstrate resilience to cybersecurity threats (see Ofwat PR19 final methodology and CAA RP3 guidance for NERL).

1. Context

Awareness of cybersecurity risks has gained momentum in the last few years with an increase in the number of cyberattacks on critical infrastructure. Such attacks are rarely brought to the public eye when they occur due to the sensitivity of the topic and the potential consequences they may have on the economy. For example, in April 2018, the Financial Times published an article about a cyberattack that was carried out over a year ago on seven of the UK's biggest banks – they were forced to reduce operations or shut down entire systems as a result of the cyberattack[3]. In May 2017, the NHS was a victim of the WannaCry cyberattack which had serious repercussions on NHS services in England, with thousands of appointments and operations cancelled[4].

These examples highlight the importance of cybersecurity, which is only going to become more prominent in the near future. This is especially relevant to energy networks as they provide critical infrastructure. MI5, MI6, the National Cyber Security Centre (NCSC, part of GCHQ) and the National Crime Agency have issued warnings on potential cyber threats to UK infrastructure, including on the UK's electricity and gas networks.

Cybersecurity also has an important international dimension given Britain's dependence on gas supplies from continental Europe and expected increases in electricity interconnection. For example, an electricity outage in one European country could have cascading impacts on other European Member States in the event one country is relying on imports from the other country affected. Similar consequences could transpire should an outage affect major gas transmission pipelines across Europe.

[3] Seven UK banks targeted by co-ordinated cyberattack. 25 April 2018. The Financial Times.

[4] NHS fights to restore services after global hack. 13 May 2017. The Financial Times.

2. Cybersecurity in the energy sector – what is being done?

In July 2016, the European Commission adopted the Directive on security of network and information systems (NIS Directive). The Directive is an EU-wide legislation aiming to boost the overall level of cybersecurity[5]. The NIS Directive was transposed into UK law in May 2018. Although not specific to the energy sector, the NIS Directive provides guiding principles and a high-level strategy for Member States to follow with regards to the security of network and information systems.

Closer to home, the UK Government published in November 2016 its National Cyber Security Strategy 2016 to 2021, which aims at making Britain secure and resilient in cyberspace. The strategy document covers different sectors important to the UK economy and alludes to the energy sector as well:

"*The rapid implementation of connectivity in industrial control processes in critical systems, across a wide range of industries such as energy, mining, agriculture and aviation, has created the Industrial Internet of Things. This is simultaneously opening up the possibility of devices and processes, which were never vulnerable to such interference in the past, being hacked and tampered with, with potentially disastrous consequences.*"[6]

Cybersecurity is also a concern for households due to the rise of interconnected and smart devices – this includes smart meters, smart thermostats, distributed energy resources, etc.

The UK Government is expected to publish energy sector specific guidance on cybersecurity in autumn 2018.

The following section discusses cybersecurity in relation to economic regulation of network companies.

[5] Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016

[6] National Cyber Security Strategy 2016-2021. HM Government. 1 November 2016, p.20,

3. Enhanced IT security in the energy sector in GB

Ofgem has recently launched an informal consultation on RIIO-1 price control 2nd re-opener. Ofgem received submissions from transmission and gas distribution companies for its 2018 window, and is expected to make its decisions by 30 September 2018.

Gas distribution companies have not requested additional allowances for enhanced security costs related to IT systems as part of the May 2018 re-opener. National Grid Electricity Transmission (NGET) and National Grid Gas Transmission (NGGT) have submitted a joint proposal for additional allowances of £72m and £53m, respectively, in 2009/10 prices for enhanced security costs related to IT systems[7]. Cybersecurity accounts for £40m of those costs, with the remainder covering enhancements to Data Centres. The requested allowances are for the remainder of the price control and are for both National Grid's Transmission Owners (TOs) and System Operators (SOs).

The full details were only provided in a confidential submission. The document in the public domain outlines the value of the allowances requested but does not provide any detail about how the money would be spent; nor does it provide details about the nature of those costs. National Grid suggests that the additional allowances will be used to implement investments which will help it achieve the key aim of the NIS Directive.

In preparing its submission for enhanced IT security, National Grid consulted with the Department for Business, Energy and Industrial Strategy (BEIS), UK Government, NCSC and external specialists in IT security to understand the potential risks and vulnerabilities present within National Grid's IT systems, property, processes and people.

Cybersecurity may be an even greater concern – and would likely account for a greater share of costs – for the SOs. National Grid's System Operator Innovation Strategy highlighted that the digitisation and decentralisation of assets require new and enhanced cyber security measures to mitigate the risk of a cyberattack[8]. This will be an important consideration as Ofgem develops the new regulatory framework for the independent electricity SO.

[7] NG Enhanced Security Reopener Public Version - May 2018. We note that "enhanced physical site security costs" is a different uncertain cost category to "enhanced security costs of IT systems". Some distribution and transmission network companies requested additional allowances for enhanced physical site security costs in both re-openers.

[8] National Grid System Operation Innovation Strategy.

3. Enhanced IT security in the energy sector in GB (cont.)

Across the RIIO-T1 period, enhanced IT security costs are likely to represent a bit less than 5% of the NGET's total controllable opex[9] or less than1% of totex.

We expect the costs related to cybersecurity to represent a growing share of network companies' cost proposals for RIIO-2 as the companies' understanding of cyber threats crystallises and they identify potential vulnerabilities.

As such, there are important considerations for how the RIIO-2 framework could deal with cybersecurity. For example, should there be a cybersecurity output? And if so, should it have a reputation or financial incentive attached to it?

Another key question is how Ofgem would account for cybersecurity in its cost assessment. Totex benchmarking models that use historical data are unlikely to be suitable for assessing companies' proposals. Bottom-up cost assessment would also be difficult as companies are likely to have varying degrees of IT security and may face different threat levels. One option would be to require additional cybersecurity cost proposals to be supported by a cost-benefit assessment (CBA). The challenge here for companies would be to establish a clear link between the costs incurred and the outcome for customers.

Given the uncertainty around cybersecurity costs, Ofgem may also wish to continue the use of uncertainty mechanisms as per the RIIO-1 approach.

Ahead of RIIO-2, network companies should develop or update their cybersecurity strategies, ensuring that they meet the objectives of the Government's Cybersecurity Strategy. This would provide a suitable basis for developing a cybersecurity work programme for the duration of the price control, and to identify the related capex and opex needs[10]. A clear cybersecurity strategy is also key for justifying any related increases in cost allowances for RIIO-2. Companies' business plans would need to demonstrate that their cost proposals are informed by a cybersecurity strategy with SMART[11] objectives.

[9] Looking at more specific cost pools within controllable opex, the requested allowances represent c. 20% of NGET's total Business Support cost or c.15% of total Closely Associated Indirect Costs over RIIO-T1.

[10] Capex in relation to cyber may include new generation firewalls, Intrusion Detection Systems, Intrusion Prevention Systems, etc. Opex in relation to cyber may include costs associated with IT security maintenance, a Chief Information Security Officer supported by an in-house cybersecurity team.

[11] SMART stands for: Specific, Measurable, Achievable, Realistic and Timely.

4. Conclusion

Awareness of cybersecurity risks has gained momentum in the last few years and is likely to feature as an important topic in energy policy and economic regulation of utilities in the near term.

Ahead of RIIO-2, Ofgem may choose to consider the regulatory approach for cyber costs. Additionally, companies may decide to enhance the interaction between their regulatory economists and cybersecurity engineers to develop well-justified requests for cyber cost allowances to be included in their business plans.

The current re-opener mechanism for enhanced security costs related to IT systems is an opportunity for Ofgem to gain knowledge on cybersecurity costs for utilities. This exercise is valuable as Ofgem will be better prepared for the next round of price control reviews; it will have a minded-to approach or position with regards to the treatment of cybersecurity costs and this may well be as part of setting ex-ante allowances.

Nonetheless, the increased focus on cybersecurity will present new challenges for both Ofgem and network companies in RIIO-2.

CEPA can leverage its extensive knowledge of the RIIO framework to help your organisation with a range of key questions regarding cybersecurity in the utilities sector:

- How should an increased focus on cybersecurity be reflected in the regulatory framework?
- How might the regulatory framework encourage collaboration between network companies on cybersecurity issues?
- Should network companies be tasked with delivering specific output related to cybersecurity? Should a reputational or financial incentive be attached to that output?
- How should cybersecurity be captured within a CBA? Including how to account for risks and hard-to-quantify benefits.

Contact us

CEPA is an economics, finance, regulation and competition advisory firm with an internationally regarded energy practice. Members of our energy team have expertise in advising both regulators and regulated companies price control strategy, development and implementation. We have extensive project experience in cost assessment, incentive design, cost-benefit analysis and regulatory finance.

Additionally, our staff and associates have extensive experience of advising a variety of stakeholders – regulators, regulated companies, suppliers and major consumers – on issues related to energy policy, market modelling and design, renewable energy support schemes and wider economic regulation topics.

Emmanuella Gentzoglanis, Senior Consultant

Email: Emmanuella.Gentzoglanis@cepa.co.uk

Emmanuella has expertise in economic regulation, policy and strategy. She has recently reviewed the RIIO framework, and network companies' performance during the RIIO-1 price controls, in order to inform Ofgem's thinking on the approach to RIIO-2. She has also advised and supported a major regulator in the Middle East with the price control of the electricity distribution companies. Prior to joining CEPA in 2017, Emmanuella worked as an economic consultant in the energy sector at KPMG.

Ben Shafran, Principal

Email: Ben.Shafran@cepa.co.uk

Ben is an experienced manager and energy policy specialist. Prior to joining CEPA in 2017 he worked at Ofgem on network regulation and was a Policy Director at the Australian Energy Market Commission. Ben has a track record of providing solutions to complex policy questions, delivering high-profile projects, and communicating clearly with a range of audiences.