



Cross-sector Resilience – Phase 2 report

Report

Publication date: 1 February 2016



About this document

The organisations comprising UKRN together provide regulatory oversight of the companies which own and operate much of the UK's national infrastructure. This infrastructure and the products and services it delivers are important, and sometimes vital, for the normal functioning of our day-to-day lives. The resilience of these infrastructures against a wide range of threats is therefore an important topic for regulators, Governments, and consumers.

This report concludes our Cross-sector Resilience project by summarising the work we have undertaken during Phase 2. The project has focussed on finding ways for the regulators to jointly tackle challenges to the resilience of UK's national infrastructure which have cross-sector implications. Most often, these shared challenges arise because multiple sectors face common threats (such as those from flooding or cyber-attack), or because of the interdependency created when the sectors rely on one another (such as the use of electricity by finance, telecoms and railway companies). During the project we have developed a new process to facilitate effective communication and coordination between us during major incidents which we are publishing alongside this report.

For further information on this work, please contact Ben Willis (ben.willis@ofcom.org.uk).

About the UK Regulators Network

UKRN is a network formed by the UK's economic regulators:

- The Civil Aviation Authority (CAA)
- The Financial Conduct Authority (FCA), including the Payment Systems Regulator (PSR) ¹
- Office of Communications (Ofcom)
- Office of Gas and Electricity Markets (Ofgem)
- Water Services Regulation Authority (Ofwat)
- Office of Rail Regulation (ORR)
- Northern Ireland Authority for Utility Regulation (Utility Regulator)

Monitor, the sector regulator for health, participates in the network and its projects as appropriate. The Water Industry Commission for Scotland (WICS) and Legal Services Board (LSB) are contributing members which generally participate in projects as observers.

Contributors to this document

This document has been produced by:

- The Civil Aviation Authority (CAA)
- The Financial Conduct Authority (FCA)

¹ Although it has competition and consumer protection functions, the FCA is not classed by HM Government as an economic regulator

- Office of Communications (Ofcom)
- Office of Gas and Electricity Markets (Ofgem)
- Water Services Regulation Authority (Ofwat)
- Office of Rail Regulation (ORR)

For further information on this report contact Ben Willis, Head of Technology Intelligence at Ofcom:
Ben.Willis@ofcom.org.uk

Table of contents

1. Introduction	4
2. Improving regulator coordination on cross-sector resilience issues	6
3. Cross-sector resilience example: electricity use in telecoms	9

I. Introduction

- I.1. In April 2015 we published the report from Phase 1 of our work under UKRN's Cross-sector Resilience project². This set out a summary of the role of UKRN members in relation to resilience, focussing particularly on cross-sectoral issues. The report also discussed a number of activities which were recommended for further work during Phase 2. The current report marks the end of this project and provides an update on the further work we have undertaken.
- I.2. There were three main areas for further work identified in Phase 1, which are discussed in Section 2 of this report. In summary:
- Cross-regulator emergency plan (CREP) – a framework setting out how UKRN members will communicate directly with one another during resilience incidents affecting two or more of our sectors. We are publishing the first version of this plan alongside the current document;
 - Joint exercise coordination – sharing information about forthcoming exercises to test response arrangements, in order to maximise opportunities for cross-sector working. UKRN members have agreed to take this forward; and
 - Cyber security assessment – working collectively and with Government colleagues to assess the level of preparedness for cyber-attacks within our sectors. This remains a very important issue and work has been progressing within individual sectors. We will continue to work individually with Government, its relevant agencies, and the newly announced National Cyber Centre³ which is expected to take a coordinating role. We do not believe additional UKRN-coordinated activity is required at this time, but we will keep this position under review as the new arrangements develop and return to it if required.
- I.3. Our last report also included a brief discussion of one cross-sector resilience issue in particular – the reliance of the telecoms sector on electricity for continued delivery of its services. During Phase 2, we have explored this issue in more detail. Section 3 summarises this work and sets out the likely impacts on a range of common consumer telecoms services in the event of different scales of power interruptions. These impacts are complex and highlight that customers should ideally consider their needs and purchase services that offer sufficient power resilience to meet them. While this may be possible for larger businesses, for consumers and smaller businesses it is not. Making an accurate assessment of their own needs will be difficult and in any case, the choice of resilience options among available products is likely to be limited. This suggests there may be a need to monitor outcomes and for possible Government intervention if the market is not delivering against any relevant objectives.

Other cross-sector resilience activity

- I.4. The majority of the resilience activity in which UKRN members are involved continues to be sector-specific, in line with our various duties, which were outlined in our Phase 1 report. Alongside this, we engage directly on specific cross-sector issues that arise and on broader sharing of information and best practice such as via Cabinet Office's Infrastructure Security and Resilience Industry Forum and various CPNI⁴-led groups.

² <http://www.ukrn.org.uk/wp-content/uploads/2015/04/Cross-sector-resilience-phase-1-final.pdf>

³ <https://www.gov.uk/government/news/chancellor-sets-out-vision-to-protect-britain-against-cyber-threat-in-gchq-speech>

⁴ Centre for the Protection of National Infrastructure – <http://www.cpni.gov.uk/>

- 1.5. UKRN itself has established an Adaptation Working Group to consider issues relating to the adaptations which companies in our sectors will have to make to deal with the effects of climate change. In particular the working group supplements the adaptation work going on within each regulator by providing a forum in which we can share information and experience on this important long term challenge to infrastructure resilience.
- 1.6. Government also maintains a strong interest in resilience matters, and this is given particular focus by the annual resilience review undertaken by Oliver Letwin MP, who as Chancellor of the Duchy of Lancaster has responsibility for the resilience of the UK's infrastructure. Further emphasis comes from an additional review led by Oliver Letwin which was announced between the various storms in December 2015⁵ and will look specifically at flooding.

⁵ <https://www.gov.uk/government/news/a-country-more-flood-resilient>

2. Improving regulator coordination on cross-sector resilience issues

- 2.1. Our Phase 1 report set out a number of areas in which we felt that additional study by UKRN members could bring resilience benefits across our sectors. This section of the report summarises our further work and conclusions on these topics.

Cross-Regulator Emergency Plan

- 2.2. It is clear from our work in Phase 1 of this project that the resilience arrangements in the different sectors vary significantly, as does each of our roles as sector regulators. However, due to interdependencies and exposure to common threats, it is also clear that there will be some incidents and emergencies which have the potential to adversely affect more than one of our sectors. The main area identified in which greater coordination between UKRN members could be beneficial to resilience was our communication when dealing with major incidents affecting multiple sectors.
- 2.3. We put forward the idea of a Cross-Regulator Emergency Plan to address this. The objective of this is to provide a more formal, but simple to use, framework setting out how we will communicate directly with one another during incidents affecting two or more of our sectors. We have developed this idea in Phase 2 of our work, and the Plan will be published on the UKRN website alongside this document.
- 2.4. The Plan is intended to sit alongside the tools for managing major incidents which already exist in each sector and centrally within Government. The Plan has been designed to be as simple as possible to maintain and use. There is no requirement for it to be used during any given incident; it is only intended to be used when one of the regulators involved feels it will be of particular benefit.
- 2.5. The unique nature of each emergency means it is hard predict the exact ways in which the prearranged multi-party communication set out in the Plan may be useful. However, from experience of similar plans that operate within particular sectors, examples might be:
- **Information sharing.** A regulator may choose to invoke the Plan if they wish to find out what the impact of an incident affecting their sector has been on other sectors or how incident response is being handled. Conversely, a regulator may have information about its own sector's impact or response which it wishes to share. This can be particularly beneficial when communicating with the companies that we regulate by improving the coordination of response across sectors.
 - **Government interaction.** There may be scenarios in which it is efficient for UKRN members to share information collectively with Government about how an incident is affecting our sectors. There may also be benefit in coordinating certain common requests of Government, such as for permission to access restricted areas to repair critical infrastructure which is used by companies in more than one sector.
 - **Public communications.** In some cases, regulators have an important role in providing information to the media and the public. In major incidents, coordination may help to ensure any messages produced by different regulators do not conflict with one another.
- 2.6. The Plan is open to all UKRN members to join. Incidents which cause a major impact across multiple sectors are relatively rare events, so we do not anticipate the Plan will be required very often. To ensure that participants maintain familiarity with it, we will undertake a simple annual exercise which

uses the Plan. Ofcom will be the owner of the Plan and as such take on responsibility for exercising and reviewing it.

2.7. The plan is published alongside this report.⁶

Joint exercise coordination

Resilience plans and exercises

- 2.8. An important part of maximising resilience is planning the response to disruptive incidents in advance. This planning might cover which aspects of a service will be sacrificed when it is under stress to ensure key aspects keep functioning, how key parties will communicate during an incident, or the order in which restoration activities will be carried out.
- 2.9. The complex nature of real incidents, as well the ever changing environment in which services exist, mean plans are rarely, if ever, perfect. Reviewing and updating existing plans and ensuring people are familiar with them are both important in ensuring they work as well as possible when they are called upon in a crisis. Undertaking regular exercises which test resilience plans can help facilitate both of these and is a common activity for most plans.
- 2.10. Government regularly undertakes exercises designed to test different aspects of the country's crisis management plans (up to and including COBR⁷), and the various department and sector-specific plans that sit below them. Exercises can take many forms, but typically involve the development of realistic and detailed scenarios, which are then "played through" by experts in relevant organisations, using the resilience plans to guide their response. This allows those that will need to use the plans in real incidents to maintain familiarity with them and for any possible improvements to be identified.
- 2.11. Most exercises will be planned by stakeholders from one particular sector. Particularly for larger exercises, stakeholders from other sectors may also be involved. For example, a recent exercise based on a flooding scenario led by the water sector, also gave the opportunity for energy and telecoms companies to participate and consider how the scenario would impact their operations.

Information sharing

- 2.12. Our Phase 1 report suggested that there may be value in UKRN members sharing information about upcoming exercises they became aware of in their sectors. This would ensure any opportunities for cross-sector participation were identified. Our work during Phase 2 has concluded that this would be useful, and could best be achieved via a simple process. When one member becomes aware of a forthcoming exercise they will consider whether there may be value in stakeholders in other sectors being given the opportunity to participate. If so, they will inform their opposite numbers in the other regulators, using the CREP contact list, along with any other regulatory contacts they think are relevant. The recipients will then decide whether and how to brief stakeholders in their own sectors about the exercise.

⁶ The Cross Sector Emergency Plan is available here: <http://www.ukrn.org.uk/wp-content/uploads/2014/05/CREP-v1.0-FINAL.pdf>

⁷ Cabinet Office Briefing Rooms. Central Government's crisis management facilities and a forum of Ministers and senior officials which makes decisions on an emergency response.

Cyber risk assessment

- 2.13. The involvement of several regulators in undertaking cyber risk assessments in their sectors was another common activity identified in Phase I. We suggested that this might benefit from UKRN-level cooperation.
- 2.14. The issue originally arose at a summit meeting involving several UKRN members and hosted by the then Secretary of State for Business, Innovation and Skills, Vince Cable. The participants at the summit committed to a number of actions, including assessing the state of cyber security across their sectors.
- 2.15. A large amount of work has been, and continues to be, undertaken in this area. Assessments, typically led by Government and the relevant security agencies, have been undertaken across a number of sectors with regulators participating as appropriate. This work forms part of the Government's Cyber Security Strategy⁸ and is expected to continue as part of the new National Cyber Security Plan⁹ recently announced by the Chancellor. Indeed, the announcement makes specific mention of the Government's intention to strengthen the regulatory framework for Critical National Infrastructure sectors in relation to cyber security.
- 2.16. It is clear that as regulators we have an important part to play in ensuring our sectors are suitably prepared to face the challenges of cyber security. However, as its recent announcements make clear, this activity will be coordinated by Government, and in particular the new National Cyber Centre which will be based in GCHQ.
- 2.17. We will all continue to work individually with Government, its relevant agencies, and the Centre as it becomes established. We do not believe additional UKRN-coordinated activity is required at this time, but we will keep this position under review as the new arrangements develop and return to it if required.

⁸ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

⁹ <https://www.gov.uk/government/news/chancellor-sets-out-vision-to-protect-britain-against-cyber-threat-in-gchq-speech>

3. Cross-sector resilience example: electricity use in telecoms

- 3.1. Cross-sector dependence can present a significant challenge to the resilience of national infrastructure. We briefly considered one example of this in our Phase 1 report – the reliance of the telecoms sector on electricity. The relevance of this example has continued to grow as consumers have shifted further towards services which typically exhibit less resilience to electricity disruption than traditional fixed voice services. During Phase 2, we have considered this topic in more detail and will summarise some of that work in this section.
- 3.2. While we have focussed on a specific example here, it is clear there are many other examples of an output from one regulated sector forming a critical input for another. Some of these relationships are two-way, creating interdependencies. Telecoms' reliance on electricity is one such example with electricity generation and distribution companies in turn using telecoms services extensively.
- 3.3. Our work has not tried to identify all these relationships as this is already an area which receives a lot of attention from other parties. Instead, this section simply gives a feel for some of the direct impacts that could be caused by one particular cross-sector dependency example. Like many other dependencies, removing it altogether is unlikely to be feasible; modifying the telecoms networks so they no longer rely on grid-distributed electricity is probably not practical or affordable. Instead, with all the current mitigations in place, the residual risk caused by the dependency needs to be understood and set against our national risk appetite. With many competing demands on the limited resources available for national infrastructure, judging whether further investment in mitigation is warranted is ultimately a matter for Government.

Resilience of telecoms to power interruptions

- 3.4. The usage of telecoms services, and the technology behind them, has been evolving rapidly over the last few decades. For many years, the only telecoms service which most consumers used was the basic fixed telephone service. This service was, and remains, very resilient to the loss of mains electricity supply because the back-up power provision within the network is usually sufficient to keep the end-to-end service operational.
- 3.5. This traditional fixed voice service is in long term decline. During 2014 for example, the volume of calls on the network dropped by 13%¹⁰. The fact that the number of consumers who have a fixed telephone line is declining at a much slower rate (0.2% over the same period) gives some comfort that in the event of a power failure the service will still be available to most people if required. However, this hides the fact that a large proportion of households have replaced all their corded phones with cordless DECT handsets. These require local mains power and so will not work during a power cut affecting a consumer's home, even if the phone service itself stays operational.
- 3.6. During 2014, BT announced its goal to move all customers off the PSTN by 2025¹¹. This network supports the majority of the UK's fixed telephone consumer services and has been doing so in its

¹⁰ The telecoms market figures in this section are drawn from Ofcom's 2015 Communication Market Review publication, http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr15/UK_4.pdf

¹¹ <https://event.webcasts.com/viewer/event.jsp?ei=1051301> – Slide 19

current form since the 1990s. While this switch off target is almost a decade away, the complexity and significance of moving away from the network is such that the project to achieve it will have to start much sooner.

- 3.7. The requirement on most fixed broadband consumers to also take a fixed phone line may go some way to explaining why the volumes of lines has not reduced at the same rate as usage. This trend of a movement towards broadband and away from traditional phone service use is seen in the mobile market too. Mobile telephone traffic saw a 2% growth in 2014, but the amount of internet traffic on the mobile networks grew by nearly 90% in the same time.
- 3.8. Within the range of broadband services, the move to faster speeds shows no sign of reducing on either the fixed or mobile networks. The number of customers buying superfast fixed broadband grew by 35% during 2014. On mobile, the latest and fastest technology, 4G, has seen a rise from 2.7 million to 23.6 million customers during 2014, largely as a result of some providers making it their standard product for mobile data.
- 3.9. These trends, particularly the move away from fixed voice and the move towards higher speed broadband on fixed and mobile networks, suggest that the most commonly used telecoms services of tomorrow will have lower levels of power resilience than those of yesterday:
 - **Fixed services.** As we discussed in our Phase I report, most of the equipment which requires electricity to deliver traditional fixed telephony on BT's network is housed in around 5,000 local exchange buildings. These are sufficiently small in number and large enough in size that they can economically house back-up power supplies sufficient to keep services running for several days during a power cut. The service is also able to supply power to consumers' homes so that corded phones will also continue to function.
In contrast, delivering superfast broadband over BT's network requires powered network equipment to be installed at around 20 times as many sites, and in the future as speeds increase further, this number may increase by another factor of 20. In addition, all available fixed broadband services include routers or hubs which require uninterrupted mains power in consumers' premises. The practical and economic challenges this presents mean future services are not expected to have the same level of power protection as current fixed telephone services.
 - **Mobile services.** The local access equipment for mobile networks, the basestations, usually have far less back-up power than fixed telephone exchanges. We looked at the reasons for this in our Phase I report. These sites are required for the delivery of voice and broadband services and so during power interruptions there are likely to be reductions in the coverage and/or capacity offered by the mobile networks.
In contrast, mobile phones themselves are battery powered and so do not require continuous mains power, although they typically need recharging on a daily basis. This is an additional measure of power resilience compared to the many fixed services with mains powered consumer equipment. The nature of mobile devices means that they can make use of neighbouring basestations if they are still powered. This may require travel to find a signal, but depending on the geographic extent of the power failure, this may be found close by or even without moving at all if the coverage of adjacent basestations overlaps sufficiently. In the case that the consumer is trying to make an emergency call, their device will use any available basestation even if this belongs to a rival network. The battery power in mobile devices therefore adds meaningfully to their resilience especially with very localised power failures which affect only small numbers of basestations.
- 3.10. While the focus above is on some challenges to telecoms resilience, it is important to acknowledge that some technology and usage changes may be beneficial for service reliability in the event of power interruptions. For example:

- The range of telecoms devices and services commonly used today creates a “strength in depth” which didn’t exist in the past. In the event of disruption to one service many consumers will have a choice of others that can form a temporary alternative.
- The use of batteries in mobile devices has been noted above as beneficial and battery technology is being used in ever more consumer equipment. For many consumers, laptops and tablet computers have replaced desktop PCs and their reliance of continuous mains power.
- While most users of battery powered devices still need regular access to mains electricity for charging, there is evidence of a trend towards demand for longer battery life, particularly in the latest generation of smartphones. This presents opportunities to increase the power resilience of a range of popular communications services.

Likely impacts

- 3.11. The following table gives some examples of the possible impact on common consumer telecoms services as a result of a range of power interruptions. In reality, the circumstances around any particular power interruption, or indeed any other resilience event, are always unique and the exact service impact is impossible to predict. For example, the table assumes there is no damage to telecoms infrastructure, but it may be that whatever caused the power interruption also damaged the telecoms infrastructure and will therefore increase the impact on services over those given here.
- 3.12. It should also be stressed that the likelihood of such power interruptions, particularly the regional and national examples, is very low. The expected impact of these more extensive interruptions is particularly hard to predict because there is little or no practical experience to draw upon.

Table 1 – Likely impacts of power interruptions on consumer telecoms services

Extent of interruption	Likely impacts	
	Fixed ^(Note 2)	Mobile
<p>Localised e.g. affecting a single telecoms site and/or small number of houses.</p>	<p>999: Service should continue, but if consumer premise power also affected, only corded phones will work</p> <p>Other Services: Telephone service from most providers should continue, but if consumer premise power also affected, only corded phones will work.</p> <p>Broadband service from most providers should continue, but in all cases will stop if consumer premise is affected by power interruption.</p>	<p>999: Service should continue if consumer is within coverage of any mobile network operator.</p> <p>Other Services: Coverage in local area may be lost or reduced^(Note 4) for customers of affected operator. If power interruption lasts beyond several hours, service from the affected site may be restored^(Note 5). Services should continue within remaining coverage of consumer’s own operator’s network, although services may be congested.</p>
<p>Small area e.g. affecting several sites, such as all basestations covering an area.</p>	<p>Broadband service from most providers should continue, but in all cases will stop if consumer premise is affected by power interruption.</p>	<p>999: Service may be unavailable across some of affected area, particularly if power interruption lasts for hours. Services should continue if consumer is within remaining coverage of any mobile network operator.</p> <p>Other Services: Coverage likely to be lost^(Note 4) in some of affected area for customers of all operators. If power interruption lasts beyond several hours, service from the affected sites may be restored^(Note 5). Services should continue within remaining coverage of consumer’s own operator’s network, although services may be congested.</p>
<p>Regional or National^(Note 1) e.g. affecting many sites and consumer premises across a whole geographic region, up to the whole country. Could last for up to 5 days.</p>	<p>999: Service should continue, but only corded phones will work. If power interruption lasts beyond several days, localised and potentially more widespread failures may start to occur^(Note 3).</p> <p>Other Services: Telephone service from most providers should continue, but only corded phones will work. Broadband service from most providers may continue, but is unlikely to be functional for most as consumer premise equipment will have lost power. If power interruption lasts beyond several days, localised and potentially more widespread failures in all services may start to occur^(Note 3).</p>	<p>999: Service likely to be unavailable across most of affected area, particularly if power interruption lasts for hours. Services should continue if consumer is within any remaining coverage of any mobile network operator.</p> <p>Other Services: Coverage likely to be lost^(Note 4) in most of affected area for customers of all operators. If power interruption lasts beyond several hours, service from some affected sites may be restored^(Note 5).</p>

Notes on Table:

¹ The national example is in line with the “Widespread electricity failure” risk included in the Government’s National Risk Register of Civil Emergencies: 2015 edition¹². This risk, which is considered very unlikely to occur, is based on a nationwide loss of electricity taking up to 5 days to restore, with some parts of the networks taking weeks for full recovery if significant damage is caused to transmission lines.

² It is assumed for all fixed network cases that individual consumers do not have any back-up power for their premises. If options such as whole-house protection or un-interruptible power supplies (UPS) for specific telecoms equipment such as DECT phones and broadband routers are in place, then the comments on premise power interruption can be ignored.

³ Most core and local exchange sites have enough onsite fuel to keep key services operational for several days. Beyond this timeframe refuelling is likely to be required and this may be affected by practical issues such as severe weather, a possible cause of the power interruption itself. If large numbers of sites are affected, such as in regional or national outages, the availability of refuelling resources is likely to be a limitation.

⁴ How quickly service will be affected will depend on the specific site(s) that have lost power, and the power protection arrangements of the operator they belong to. The majority of basestation sites have either no power back-up, or just enough to last for a few minutes, typically not intended to offer continuing service, but rather to allow the equipment to shut down properly when mains power is interrupted.

Some operators install additional back-up power facilities, typically able to maintain normal operation for between 1 and 8 hours, at a limited number of “key sites”. These may be sites which provide onwards transmission to other sites and/or coverage for critical users or locations.

⁵ Power restoration is dependent on portable back-up power being deployed to the affected site(s). Practical issues such as severe weather, which may be associated with the power interruption itself, may delay or make impossible this deployment. If large numbers of sites are affected, such as in regional or national outages, the availability of such resources is likely to be a limitation. For sustained power interruptions (e.g. lasting for days), refuelling of the back-up power supplies is likely to be required, and again this will be subject to practical and resource constraints.

3.13. The table shows that even small power interruptions can have a knock-on impact on telecoms services and severe disruption can occur in some cases. Power interruptions are of course only one of many possible threats to the availability of telecoms services. The table above also focusses just on the most common consumer services and even then simplifies them considerably to just a few categories. In reality, different customers will use different combinations of services and place different levels of importance on their continued operation during a range of incidents.

3.14. This high level of real world complexity therefore makes a question such as “how reliable are telecoms services” impossible to answer in the abstract. The practical advice for all telecoms customers is to consider their specific resilience requirements and purchase services which meet these.

3.15. For larger businesses, their spending power and expertise mean that this is a realistic option. They are able to devote sufficient resources to establishing their exact needs and purchasing services tailored to them. However, for small businesses and consumers this is less likely to be the case. They will usually be able to choose from only standard off-the-shelf services with a limited range of resilience options.

¹² https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/419549/20150331_2015-NRR-WA_Final.pdf#page35

They are also less likely to be able to assess how well these will meet their resilience needs or indeed to perform an accurate assessment of exactly what their needs are.

- 3.16. This suggests a need to monitor the resilience of telecoms services to power interruptions and how well this fits the needs of customers as technology and usage continues to change. This need is reinforced by the trend for telecoms to play an ever more important role in the smooth running of our economic and social lives. If there are shortfalls in the market's delivery of sufficient power resilience for particular services, whether they are used for accessing the emergency services or continuing more routine internet activity, Government intervention may be required.