Climate Change Adaptation for the ICT sector

1 What is climate change adaptation?

Adaptation is all about assuming that climate change will happen and being resilient to the impacts. It differs from mitigation which is all about finding ways to minimise climate change by reducing carbon emissions. Mitigation is therefore about trying to *prevent* climate change and adaptation is about *coping* with it.

Adaptation can take different forms: We can adapt to climate change by retrenching (the "living in caves and eating bugs" option) but what we really want is to continue to enjoy our current quality of life. To do that we must make sure that the complex support systems that we rely on can still function adequately when climate change risks are realised. This means that those systems – our infrastructure - must be resilient to climate change risks in the same way that we try to make them resilient to other forms of interference such as theft, vandalism or terrorism: if our infrastructure is compromised then so too is our economic and social activity.

Building infrastructure resilience is tricky. Firstly, climate change risks are uncertain and so are hard to plan for and secondly improving resilience costs money. That said, it is neither necessary nor practical to plan for complete resilience: the important thing is that climate change risks are recognised, prioritised and managed appropriately.

2 ICT and the Adaptation Reporting Power (ARP)

The 2008 Climate Change Act not only addressed mitigation but also set out a policy strategy on adaptation. This gave DEFRA the power to require those responsible for our critical national infrastructure (CNI) to report formally on their climate change readiness on a regular basis. In this first round, reports were due in 2011. Obliged infrastructure providers included water, electricity, highways, railways, national parks and ports among others. Although communications are considered part of the CNI the incumbent telecoms provider was not obliged to report, but was invited to report voluntarily. Other aspects of ICT provision (i.e. data centres) were not considered for inclusion in the first round of reporting.

Prior to the second round of reporting, techUK observed that digital infrastructures were missing from government assessments of the CNI and that this omission could undermine resilience planning because of interdependencies between infrastructures, many of which now heavily depend on ICT. techUK was subsequently invited to report on behalf of the ICT sector and this report, due in 2015, will focus on data centres as providers of the core digital infrastructure that underpins most if not all modern economic activity. Telecommunications represent both core and distributed parts of the ICT infrastructure and will be reported on separately under communications by the incumbent provider as well as by OFCOM. The two reports will be coordinated and cross referenced.

3 Assets vs. processes

Traditionally attention has been focused on managing physical assets and physical infrastructures (eg adapting the specifications of a new bridge to accommodate higher water levels or resist stronger currents and other erosive forces). However, we live in a service economy. Modern business processes are all about service delivery, whether that service is providing a tasty sandwich, supplying electricity or getting people to work on time. Infrastructure operators are essentially service providers and need to plan their adaptation strategies from a service delivery perspective. They need to find ways to maintain their regulatory obligations and meet customer expectations even when climate change risks are realised. Adaptation strategies therefore have to build resilience in both physical assets and in business processes.

4 What are the main climate change risks relevant to ICT infrastructures?

Climate change risk scenarios are set out in UKCP09 (UK Climate Projections 09) which provides scenarios of climate change impacts of different levels of severity and likelihood between 2010 and 2099 in three overlapping periods. UKCP09 has recently been revisited in the light of recent weather conditions and is still valid, hence the absence of a more recent set of projections.

The challenges posed by climate change fall into two main categories: acute events and chronic stresses. Acute events (also termed critical or crisis events) include floods (pluvial, fluvial, coastal), hurricanes, ice storms, heatwaves, etc. Acute events compromise infrastructures by destroying or disabling the physical assets that they depend on. While they may have devastating effects, acute events tend to be short-lived.

Chronic stresses result from more gradual changes in climate norms. These changes include increased diurnal and annual temperature ranges, greater exposure to temperature extremes, longer sustained high temperatures, more rapid temperature variation, higher humidity and second order effects such as changes in patterns of precipitation and wind leading to more frequent water ingress or storm damage. While these impacts are less likely to have catastrophic consequences, they will lead to faster asset degradation, more frequent failures and shorter life spans which in turn will have significant financial consequences because assets will need more frequent upgrade and replacement cycles and probably require more intense monitoring for signs of deterioration. Chronic stresses manifest themselves over much longer timeframes.

These two types of stress are not discrete: a third type of stress has been identified as a "chronic crisis[1]" or "chronic hazard condition", essentially an acute event sustained for a significant period of time (eg. flooding that lasts for weeks or months instead of days – such as that experienced in 2012).

5 Key climate change impacts relevant to ICT infrastructures

Climate change risk is now viewed as business risk. Risk assessment has to differentiate strategic risk from operational risk, risk to assets from risk to business processes. It also has to balance the cost of improving resilience against risk horizons. All approaches should accept that some degree of failure is inevitable.

a) Impacts of climate change on physical assets

See table 1 below

b) Impacts of climate change on service delivery

i. Difficulty in meeting regulatory obligations (telecoms)
ii. Interruption to customer services and consequent requests for compensation
iii. High customer call rates to contact centres and helplines
iv. Concerns over staff wellbeing
v. Reputational damage
vi. Unbudgeted financial costs
vii. Resources diverted from scheduled activities with consequent second tier disruption

Table 1: Climate change impacts on Physical ASSETS

Climate change risk	Type of impact	Implications for communications infrastructure	Implications for data centre operations
Flooding: coastal	Erosion	Exposure of cabling, Damage to materials, Exposure of foundations, Subsidence	Exposure of cabling, Damage to materials, Exposure of foundations, Subsidence
	Inundation by salt water Increase in salt spray	Water damage to assets such as cabinets, ducts, and to exposed infrastructure. Salt damage to assets, disruption to transport networks and fleet operations	Water damage to assets such as cabinets, ducts, and to exposed infrastructure. Salt damage to assets, disruption to transport networks.
Flooding:	Erosion	Exposure of cabling, Damage to	Exposure of cabling, Damage to

[1] Guppy, L. Twigg, J. in Environmental Hazards, Benfield Hazard Research Centre, UCL. (See Bibliography)

fluvial		materials, Exposure of foundations, Subsidence	materials, Exposure of foundations, Subsidence
	Inundation by fresh water Silt deposit	Water damage to assets - cabinets, ducts, exposed infrastructure, silt damage to assets, disruption to fleet operations	Water damage to assets - exposed infrastructure, silt damage to assets, disruption to transport
Flooding: pluvial	Flash floods – inundation of localised area	Water damage to cabinets, ducts, exposed infrastructure and above-ground infrastructure, disruption to local transport & fleet operations	Water damage to exposed infrastructure and above-ground infrastructure, disruption to local transport
	Large droplet - Greater force and penetration	Damage to connection points eg at top of poles, water ingress to cabinets	Unlikely to be significant
Drought	Changes in water table, shrinkage of subsoil, changes in shear strength of subsoil	Subsidence damage to masts, poles and other built infrastructure, fractured ducts	Water shortage may impact cooling functionality in some facilities
Increased storminess	High wind speeds and gusts, higher likelihood of storms	Damage to aerial infrastructure, telegraph poles, masts. Damage from other objects hitting wires and poles (eg falling trees) Damage to cabling due to heave from tree roots. Disruption to fleet operations if roads are blocked.	Damage to buildings, damage to underground cabling (if trees uprooted), disruption to transport if roads are blocked. Other second level interdependencies.
Increased humidity	Moisture penetration and retention	Damage to exposed assets	More active humidity management required. higher risk of damage to hardware
High summer temperatures	High internal temperatures in cabinets, exchanges and data centres	HSE issues for staff. Heat stress on assets. Increased cooling requirements in exchanges and data centres.	Sustained temperatures present significant challenges for legacy sites in particular. May compromise activity if cooling cannot be maintained.
Changes in temperature ranges	Wider diurnal temperature ranges	Assets have to function reliably over a wider temperature range.	Assets have to function reliably over a wider temperature range. Impacts on cooling provision and temperature management
	More rapid temperature change	Greater stress on components and connections.	Greater stress on components and connections, impacts on cooling provision.

6 Barriers to building resilience

Most operators have identified similar barriers, many concerned with the regulatory constraints they operate under and the difficulty of making a business case for investment or in convincing customers that investment is necessary for uncertain risks. The most obvious barriers are listed below.

a) Difficulty in evaluating risk: Inherent uncertainty of climate change risks

b) Problems of establishing cost benefit analysis / building a business case for improving resilience

c) Convincing senior management / shareholders /customers that adaptation actions are required

d) Incompatible decision cycles (eg regulatory price reviews vs. climate change horizons)

e) Accessibility / usability of data/ issues with Environment Agency data

f) Difficulty in differentiating climate change risks from BAU weather risks

g) Difficulty in setting risk thresholds

h) Difficulty in prioritising risks (lack of data / data collection only started recently)

i) Applying climate science, especially UKCP09.

j) Interdependency (dependence on other sectors or third parties)

k) Addressing the current focus on assets rather than processes

l) Extracting relevant data from existing fault reporting processes

m) The tendency to try to protect everything

7 Interdependencies

ICT is heavily dependent on electricity. Second order dependencies include:

- Fuel supply for back-up generators in exchanges and data centres: in general, guaranteed service levels are in place for emergency fuel provisioning.
- Transport – disruption to transport networks (interruption in fuel supply and damage to roads) will have impacts on fuel delivery

In theory, for IT function to fail on a large scale, both electricity and transport would have to be severely disrupted – ie that grid power is unavailable for a sustained period of time and transport links are disrupted enough to prevent emergency fuel deliveries.

Data centres can operate indefinitely on back up generator power but would then rely on deliveries of gasoil which in turn rely on the transport infrastructure being operational. However, much critical data centre infrastructure is duplicated or mirrored or otherwise backed up at different geographical locations so a loss of functionality at one site would not necessarily result in disaster.

A scenario in which mains electricity is unavailable and transport links dysfunctional over a sustained period *and* geographical area may seem the province of only the most neurotic of contingency planners but this situation occurred recently in New York as a result of Hurricane Sandy. More significantly one back-up site was disabled because both primary and secondary sites were within the 400 mile impact zone of the storm. On that occasion, some data centre customers had to fall back their own contingency arrangements.

8 Summary of key adaptation issues for ICT

At a physical level our distributed communications infrastructure presents a very different set of challenges to resilience planners than the core digital infrastructure represented by data centres. At a service delivery level, however, the differences are much less distinct.

Another key difference is regulatory constraint: communications are regulated through OFCOM whilst data centres are not similarly regulated as an industry sector (although of course operational aspects are covered by numerous regulations). Absence of a sector regulator is unlikely to compromise data centre resilience – market forces ensure that data centres compete around operational resilience – as even the most cursory examination of the sector will demonstrate. In fact, regulated sectors almost universally report that their regulatory obligations often handicap their efforts to improve resilience. Some regulators for instance will only consider risks applicable to the period covered by the current Price Review. In communications some of the provisions of the USO make it harder to manage climate change risk cost-effectively.

9 Further Reading

The adaptation literature is well developed and we reviewed it in 2013. There are, however, few publications that cover adaptation in relation to ICT. We also have access to brief adaptation best practice case studies relevant to the sector but we would need to seek permission before sharing these.

10 Contacts

Emma Fryer, Associate Director, Climate Change Programmes: emma.fryer @techuk.org