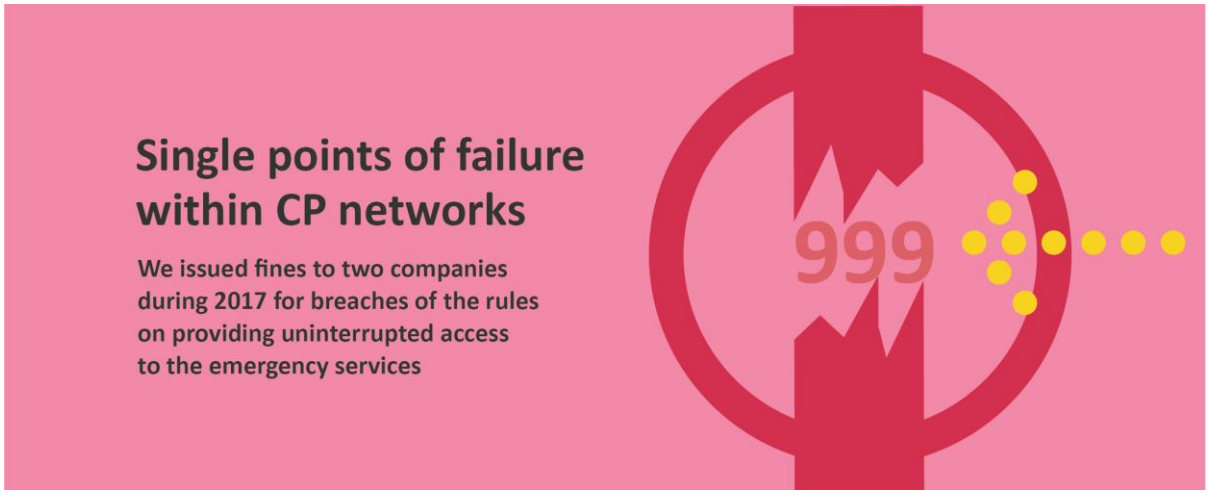
8. Security and resilience

Overview



8.1 The security and resilience of fixed, mobile and broadcast television networks and services is increasingly more important. This section summarises the major security and resilience issues that were reported to us over the past year along with some key themes from the work we have done over the past year.

8.2 Important points to note are:

a) Most security incidents reported relate to voice services, often affecting consumer access to the 999 emergency services;

b) The majority of incidents are caused by the failure of hardware components, the loss of power supply or by software bugs;

c) We are reporting more incidents on mobile networks as a result of our ongoing effort to improve the reporting of mobile incidents;

d) Cyber attacks on telecommunications networks have the potential to have very serious consequences. Working under existing and new legislation in this area, we are increasing our focus on this security threat.

e) Two investigations into the resilience of voice access to the emergency services have concluded in the last 12 months, both with fines for the providers involved. This has highlighted the importance of ensuring appropriate resilience measures are in place;

f) The resilience of mobile networks, in particular to major power disruption, remains a key concern; and

g) Further to the overview of issues associated with the so-called “PSTN switch off” we noted in last year’s Connected Nations report, we have established a programme of work with providers and other stakeholders that is aimed at identifying and mitigating any consequent risks to consumers.

Our role in security and resilience

Ofcom and providers of communications networks and services are subject to certain requirements.[93] These include requiring operators to appropriately manage security risks, to minimise impacts on consumers and to report any breaches of security or network failures to us.

We first published guidance on the full range of security requirements in May 2011 and updated that guidance in August 2014.[94] We are in the process of further updating the guidelines. The guidance sets out our expectations for a risk-based approach to the management of security. It highlights appropriate sources of industry best practice and details our incident reporting requirements.

Aside from these specific requirements, digital terrestrial television (DTT) operators have an obligation[95] to meet high standards of reliability and to provide us with an annual report on transmission performance.

DCMS has recently concluded a consultation on introducing new legislation to implement the EU's Network and Information Systems Directive. This will extend similar security and resilience requirements to a number of additional infrastructure sectors. Under the new legislation, we expect to take on additional responsibilities in relation to providers of certain essential internet infrastructure.

Resilience of fixed and mobile networks

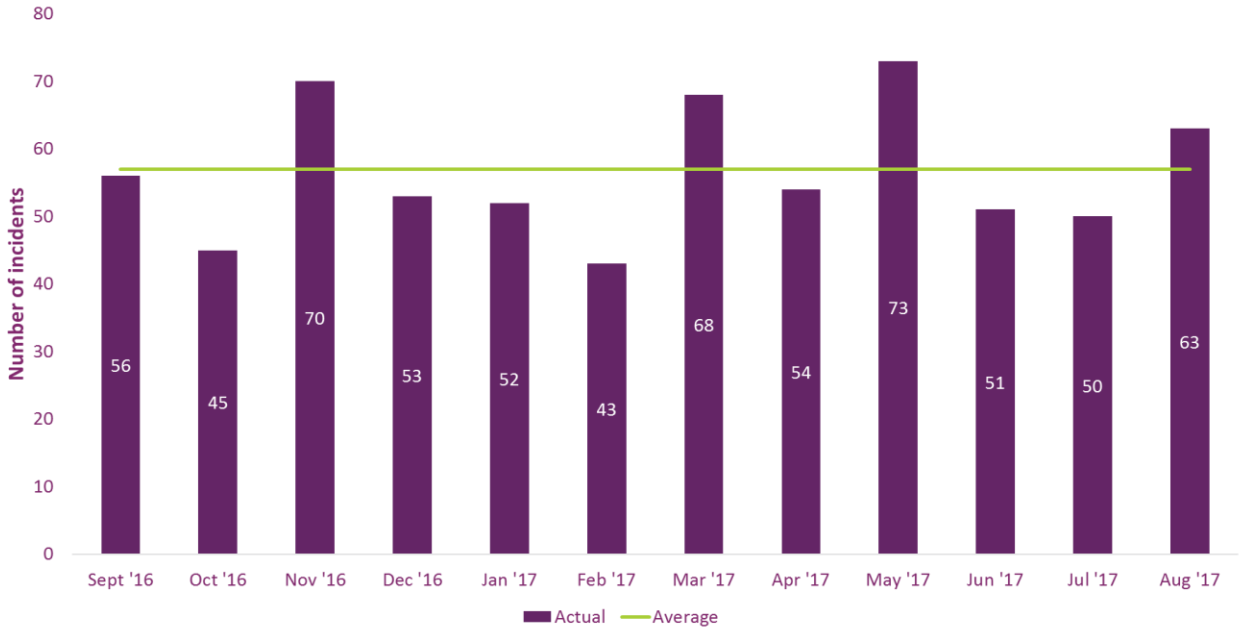
Most security incidents reported relate to voice services, often affecting consumer access to the 999 emergency services

8.3 In the past year, 678 security incidents were reported to us by fixed and mobile providers. Most reports were from fixed providers regarding disruption to telephony services (including 999 access) for fewer than 10,000 customers and for less than one day. Incidents with a wider impact, which affect tens of thousands of customers, are less common. Reporting data also show that incidents are more likely to occur in, or near, large population centres.

8.4 Figure 38 summarises the number of incidents reported each month between September 2016 and August 2017. The monthly variation could be the result of seasonal factors, although we note there is little, if any, correlation with the variations seen in last year's report. We continue to monitor for trends over time.

[93] In accordance with Article 13a of the Framework Directive[93], sections 105A-D of the Communications Act 2003 place requirements on providers and Ofcom regarding the security and resilience of communications networks and services.
[94] http://stakeholders.ofcom.org.uk/binaries/telecoms/policy/security-resilience/ofcom-guidance.pdf
[95] http://stakeholders.ofcom.org.uk/binaries/broadcast/guidance/techguidance/tv_tech_platform_code.pdf

Figure 38: Number of incidents reported between September 2016 and August 2017



Source: Ofcom analysis of operator data

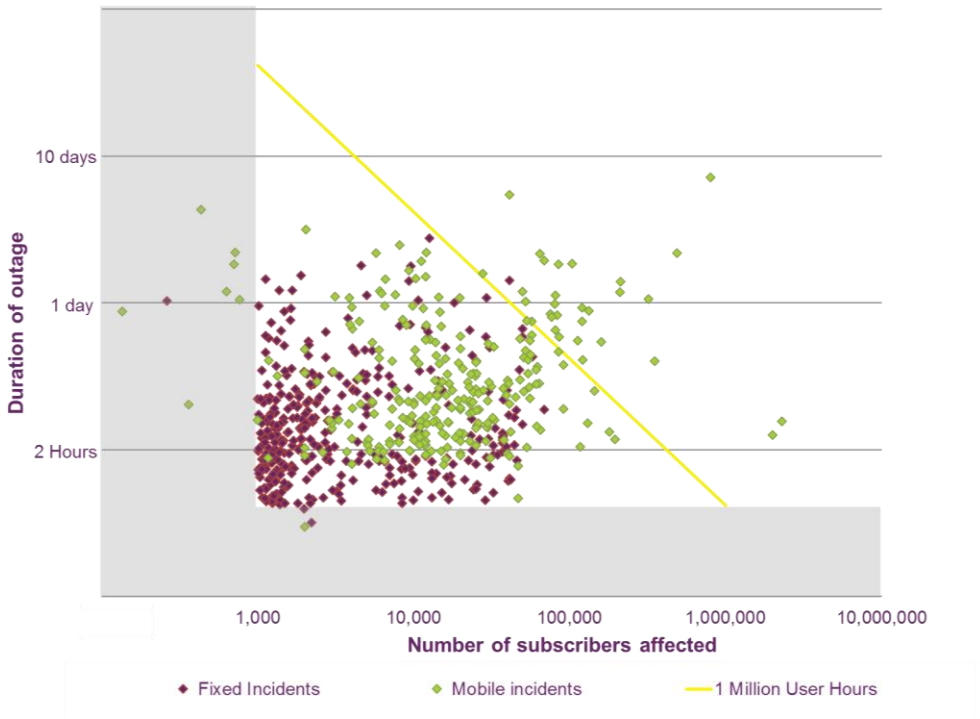
Framework for incident reporting

8.5 Our guidance provides quantitative criteria, or thresholds, against which a provider can gauge the impact of an incident and determine if it should be reported. The most critical is the 'emergency services access' threshold which applies to incidents that affect voice access to the emergency services for 1000 customers, for one hour. There will be incidents that occur, but which are not reported to us, since they do not have 'significant impact' as defined in relevant guidance.

8.6 We measure the impact of an incident in 'customer-hours'. This is the product of an incident's duration and the number of consumers affected. While customer-hours is not the only metric by which incidents may be measured, it provides a useful basis for comparison.

8.7 The majority of incidents have a relatively low customer-hours impact and are reported under the 'emergency services access' threshold. Figure 39 shows the customer-hours impact of the 678 incidents that were reported to us.

Figure 39: The impact of incidents reported to Ofcom, between September 2016 and August 2017



Source: Ofcom analysis of operator data

Changes in the reporting of mobile incidents

8.8 Our current guidance, published in August 2014, places a particular emphasis on receiving more incident reports from the mobile sector, given the growing importance of mobile services to consumers.[96] At the time, we decided to set reporting thresholds individually with each of the four main mobile network operators. This approach was intended to arrive at similar reporting thresholds for each operator, but in a way which reflected how they each detected and responded to major incidents, hence minimising any unnecessary reporting burden.

8.9 However, we are concerned that the current thresholds for reporting of incidents affecting mobile services are resulting in significant differences between the MNOs in deciding which incidents should be reported and how their impacts should be calculated.

8.10 We have been working with MNOs to address this issue, and this has resulted in a significant increase in reports in some cases, but not all. Between September 2016 and August 2017, 298 mobile incidents were reported compared to just 33 in the previous reporting period.

8.11 The new reporting methodologies being tried by the MNOs have also affected how the impact of some incidents are calculated. It is inherent in mobile incidents that mapping between the affected infrastructure and the impact in terms of geographic area, the

[96] https://www.ofcom.org.uk/__data/assets/pdf_file/0021/51474/ofcom-guidance.pdf

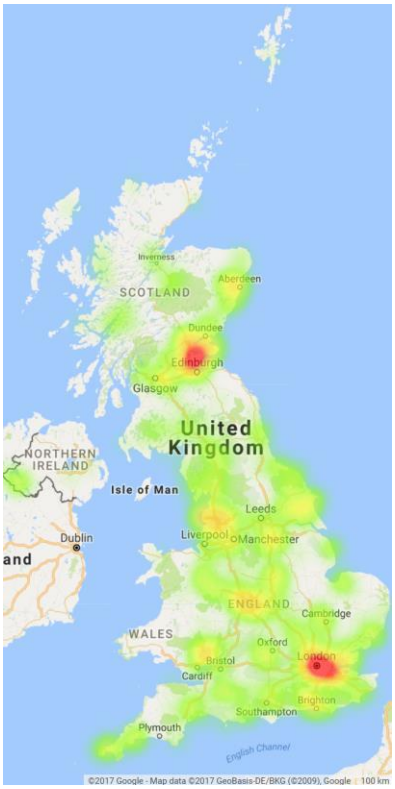
number of customers, and the service impact, is an estimate, rather than a precise calculation. We believe that the apparent increase in major mobile incidents is a result of these new attempts to more accurately estimate impact, rather any underlying deterioration in the reliability of mobile networks.

8.12 We recently consulted on another revision to our published guidance.[97] Our proposals include adopting new mobile reporting thresholds and more prescriptive guidance on how customer impact is calculated. The consultation has closed. We will be considering responses and, in light of these, will decide on whether to adopt a new mobile reporting regime to further improve the quality and consistency of data we receive.

8.13 Figure 40 shows how the 678 reported incidents are geographically distributed across the UK, and reveals that there is a correlation between incident frequency and population density. Where population densities are higher, a higher concentration of network equipment, or assets, is required to provide services.

8.14 It is logical to expect that, where there are more assets, there is a greater likelihood of incidents. However, our minimum incident threshold of 1,000 end-users affected may result in some rural incidents not being reported.

Figure 40: Heat map showing the distribution of incidents throughout the UK



Source: Ofcom analysis of operator data

[97] https://www.ofcom.org.uk/consultations-and-statements/category-1/review-security-guidance

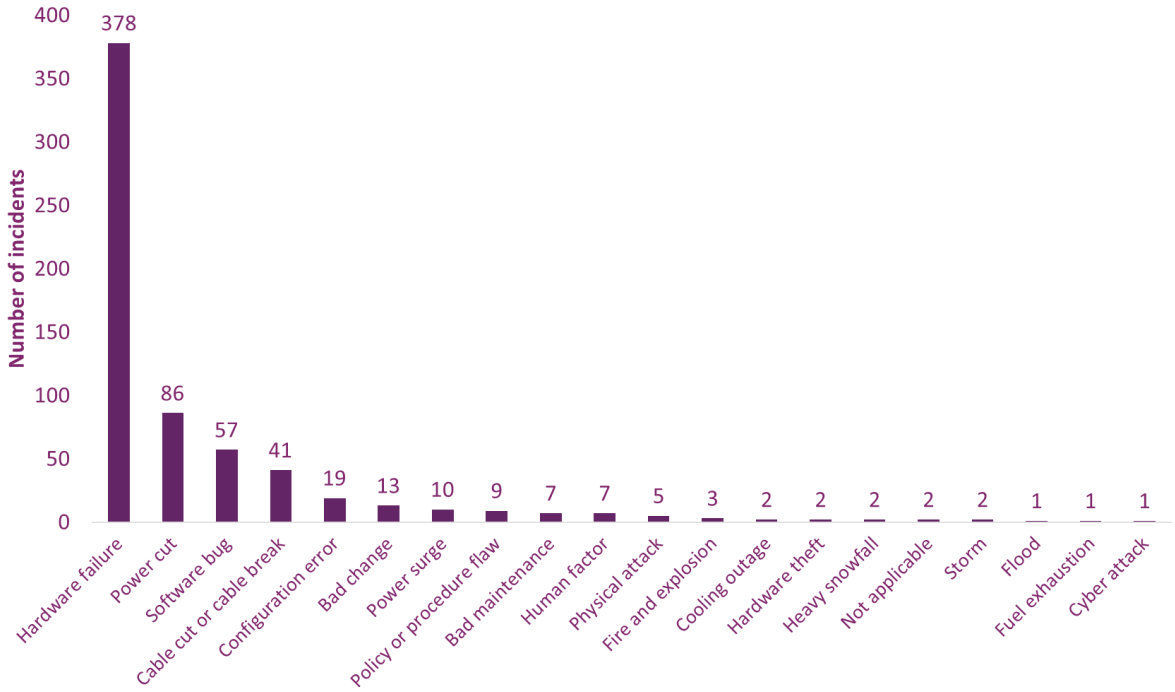
Most incidents are caused by the failure of hardware components, the loss of power supply, software bugs or cable problems

8.15 Establishing the root causes of incidents is central to understanding risks to the security and resilience of networks and services. There are four broad categories of root cause used in reporting at a European level. Of these, system failure is overwhelmingly the main root cause of significant network incidents; over 93% of reported incidents fall into this category. This includes hardware and software failures, and the failure of systems, processes and procedures.

8.16 The remaining categories are human error, natural phenomena (which includes severe weather) and malicious actions, which were responsible for 4%, 2% and 1% of the reported incidents, respectively.

8.17 Figure 41 shows that incidents were reported against a wide range of primary causes.[98] 'Hardware failure' is the most common primary cause, followed by 'power cut', 'software bug' and 'cable break'. Together these causes account for over 86% of the incidents that are reported to us.

Figure 41: Primary cause of incidents reported to Ofcom, September 2016 to August 2017



Source: Ofcom analysis of operator data

[98] We categorise the root and primary cause of reported incidents according to the taxonomy provided in the ENISA Article 13a Technical Guideline on Threats and Assets, https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets

We are concerned about the dependence of lifeline services on mains power

8.18 Traditional corded telephones are powered over the copper line which runs from the local exchange, and this makes it possible for people to make emergency calls from their home even when there is a power cut. This is important, given the possibility that a power cut is associated with some other event which means people need to call for help. However, as traditional corded telephones are replaced by new types of telephone (wireless handsets, devices which enable telephone calls over broadband), and as copper exchange lines are replaced by fibre, this facility may no longer be available.

8.19 We recognised the importance of this issue in our Strategic Review of Digital Communications. We need to protect people's ability to access lifeline services, whilst giving operators flexibility to do this in a manner that does not hold back investment and innovation in new services. We therefore stated we would assess what operators are doing on a case-by-case basis provided the technical solution delivers a level of protection equivalent to that provided by traditional means. We continue to engage with operators on this basis.

8.20 We also believe that more needs to be done to improve the resilience of mobile networks in the face of electricity supply failure. Mobile networks are increasingly used as a means of safety-critical communications, in particular around 70% of 999 calls are now made on a mobile phone. This dependence of lifeline services on mobile networks is likely to increase over time. However, mobile networks generally rely on mains electricity more than 'legacy' fixed telephone networks. We will work with both industry and government to identify options for improvement.

8.21 We plan to include data on power resilience in our next report and to ask mobile network operators for information about their primary and back-up power arrangements at cell and core sites.

Cyber Security

Although reported cyber attacks are rare, they have the potential to cause serious impact

8.22 As shown in Figure 41, very few of the reported incidents of significant service interruption over the past year were attributed to a cyber attack. However, this does not mean that cyber attacks on telecommunications networks do not occur, nor that they can't have very serious consequences.

8.23 The public profile of cyber security incidents has grown in recent years. The motivations behind cyber attacks vary from nuisance and petty vandalism, through varying levels of criminality, up to activities attributed to hostile nation states. Telecommunications networks are often involved, sometimes as conduits for the attack, but also sometimes as the targets. Typically, however, the motive of a cyber attacker is not to cause an outage to the telecommunications service itself, which goes some way to explain why so few such

incidents hit our numerical reporting thresholds. More often, the attacks are intended to steal personal or business data, or to disrupt applications using the underlying telecommunications services, such as websites.

8.24 The consequences of such attacks can be significant, both for any communications provider involved as well as their customers. The TalkTalk incident in 2015 is probably the highest profile attack directly on a telecoms operator. TalkTalk's telecommunications services themselves were essentially unaffected. However, customers were potentially exposed to financial fraud and identity theft, and TalkTalk received a fine from the ICO as well as financial, reputational and share price losses.

8.25 There is the potential for much more serious consequences from a cyber attack on telecommunications. Many of our telecommunications networks form part of the UK's critical national infrastructure – systems on which the country's smooth economic and social functioning relies. Cyber attacks intended to damage or disrupt these networks could clearly be very serious, and this is one of the reasons Government has placed so much focus on improving our national defences.

Existing obligations on communications providers include cyber security and we are increasing our focus on this area

8.26 Under s105A, the Communications Act 2003 requires providers to take measures to manage risks to security and availability of their PECN and PECS.[99] It does not limit the types of threats that should be considered and therefore measures to manage cyber threats, such as cyber attack, should be included. As such, we have written to the major providers about our expectations in relation to cyber security and included the issue in our bilateral discussions.

8.27 We publish compliance guidance for providers[100], and this identifies the importance to the UK of cyber security and the central role of providers. It also sets out several Government cyber security initiatives that are relevant to the security measures that should be considered under section 105A. Over the summer, we consulted on updating this guidance[101] and cyber security is one of the areas in which we have proposed changes to reflect our increasing focus.

8.28 An important part of this focus has been working with DCMS on a project it has been leading to develop a cyber vulnerability testing framework for providers. This will assess the real-world level of cyber-defences that providers have put in place, and is modelled on the CBEST[102] scheme which the Bank of England has been operating for financial institutions for several years. Under the scheme, detailed intelligence is gathered on the threats faced by the provider undergoing testing, and forms the basis for various penetration tests undertaken on its operational networks. As well as assessing how well

[99] Public Electronic Communications Networks and Services
[100] https://www.ofcom.org.uk/__data/assets/pdf_file/0021/51474/ofcom-guidance.pdf
[101] https://www.ofcom.org.uk/consultations-and-statements/category-1/review-security-guidance
[102] http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx

defended the provider's network is against such attacks, such testing also shows how well it could detect and respond to any successful attempts.

8.29 We believe such a scheme has great potential to increase both the level of cyber security that providers have in place and the level of assurance among ourselves and Government of providers' ability to defend against and respond to attacks. We also consider that this approach would be more effective than reliance on security standard certification alone.

8.30 The scheme is now undergoing a pilot phase. We will consider using it as part of our assessment of s105A compliance when this is complete and a suitably robust testing framework becomes available.

The Network and Information Systems (NIS) Directive is expected to introduce additional obligations when it comes into UK law in 2018

8.31 The NIS Directive is due to be transposed into UK law in May 2018. Among other things, it will extend similar obligations to those in s105A to operators of critical infrastructure in other sectors, and has a particular focus on cyber security threats.

8.32 Under the current Government proposals, we will take on responsibility for enforcing the NIS Directive for companies in the 'Digital Infrastructure' sector. This includes major providers of domain name system (DNS) services, domain name registries, and internet exchange points (IXP).

Ofcom will continue to work closely with other relevant bodies

8.33 Cyber security is a complex and very technical area. As such, we, in common with other sector regulators, will require support from National Cyber Security Centre (NCSC), the recently established UK authority on the subject. NCSC has a defined role as the 'Technical Authority' under the NIS Directive, and is expected to coordinate incident reporting.

8.34 We already have strong links to NCSC via its predecessor organisation, and will continue to develop this, and our methods of sharing information and working together, to support both our NIS and s105A activities.

8.35 The connection of many cyber security incidents to personal data loss means that we will also need to continue our close working relationship with the Information Commissioner's Office (ICO). ICO are also expected to have an important role in relation to Digital Service Providers (such as online marketplaces and cloud computing services) under the NIS Directive, so again cooperation will be required.

8.36 Many other organisations and departments have an interest in cyber security, such as National Crime Agency, DCMS and Cabinet Office. We will continue to build our relationships with them, as well as own cyber capabilities.

Single points of failure

Two recent investigations have highlighted the importance of avoiding single points of failure

8.37 We issued fines to Three and KCOM during 2017 for breaches of the rules on providing uninterrupted access to the emergency services.[103] In both of these cases, we concluded that the companies hadn't taken sufficient steps to avoid single points of failure in their networks.

8.38 By single points of failure, we mean instances in which the network relies on significant amounts of traffic passing over a single route, a single point of handover, or on routing through a single location, which leaves specific points of vulnerability within a network. We have no reason to think that two such findings in one year indicate any broader issues within the sector. However, the incidents do offer a reminder of the importance of ensuring sufficient network resilience.

We will be paying particular attention to this issue in our future enforcement work

8.39 The level of network resilience that is 'sufficient' will vary depending on a number of factors. The type of service being offered is one. In both the cases mentioned above, it affected 999 access services, which we hold to the highest standards. As such, communications providers are required to take all necessary measures to maintain, to the greatest extent possible, uninterrupted access to emergency organisations. This means we expect them to do everything technically feasible and within their reasonable control to ensure sufficient resilience.

8.40 In general, providers should avoid single points of failure where it is reasonably possible to do so. The extent to which avoiding single points of failure is reasonably possible will vary at different points in the network and in different circumstances. Various factors need to be taken into account, for example:

- the number of customers relying on the single point of failure, with more customers justifying greater efforts;
- it is more likely to be disproportionate to deploy protection paths (and hence avoid single points of failure) in the access network than in a provider's backhaul and core networks; and
- any geographic and physical constraints.

[103] https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2017/three-fined-emergency-call-service-failure and https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2017/kcom-fined-900,000-for-emergency-call-failure

8.41 In our recent consultation on updating our section 105A guidance, we have noted this issue as one we will give particular attention to in the future. We have proposed making changes to the guidance to reflect this.

The future of voice services

8.42 Historically, voice services have been predominantly provided by a dedicated switching and signalling network (the Public Switched Telephone Network, PSTN), supported by copper wire access to the home and requiring specific end user equipment in the home (i.e. a telephone). However, this model is seeing substantial change:

- The PSTN is now approaching its end of life. Globally, it is becoming increasingly difficult to maintain them, as the availability of spare parts and the engineering knowledge to effect repairs reduces;
- The fixed access network itself is moving away from copper wire access to fibre technology;
- In many new-build housing developments, where providers are already deploying full fibre broadband services, residents are already using VoIP;
- Mobile networks are becoming the platform of choice for voice services – they now carry over twice as many 'voice minutes' as fixed networks[104]; and
- Consumers are adopting IP-based voice-capable communication services (e.g. Skype, WhatsApp) which are agnostic to the underlying network or end-user equipment and usually offer additional features such as messaging or photo and video sharing.

8.43 In last year's Connected Nations Report[105], we noted these trends and outlined our then understanding of their implications and the policy principles we would seek to apply in considering market and service developments. Since then we have been in dialogue with most of the leading providers about their plans and have established an industry working group with wider stakeholder participation to consider the issues arising.

8.44 Providers that currently operate PSTN infrastructure are looking to retire this network and deploy an 'All-IP' based core network. For many consumers their service provider will offer a new broadband router or set-top box that combines both broadband and phone services. Integrating the voice and data services in this way offers a high degree of flexibility and functionality to consumers, including the potential to switch seamlessly between the underlying access networks (fibre, cable or mobile).

8.45 Different providers are at different stages of managing this process, with the particular approach adopted by each and the timescales over which any migration takes place also potentially differing. Some providers, such as Virgin Media with its Project Lightning network expansion progamme, are already deploying 'All IP' voice solutions to new customers connected to their newly deployed infrastructure. We would expect to see

[104] See p130 of the UK Communications Market Report 2017.
https://www.ofcom.org.uk/__data/assets/pdf_file/0017/105074/cmr-2017-uk.pdf
[105] See sections 7.18 to 7.44 of Connected Nations 2016

initial migrations for existing customers on traditional PSTN connections to start taking place over the coming year both as a result of new infrastructure deployment and from the launch of Openreach's 'SOGEA'[106] upstream wholesale product to retail service providers. SOGEA allows broadband-only products to be supported over Openreach's network, which may incentivise providers to offer voice services over broadband rather than as a separate service.[107] Under providers' current plans, we would expect migration to be complete by the middle of the next decade.

Migration to the new services will bring benefits to consumers

8.46 Moving voice services to broadband, away from traditional analogue access network delivery, means that new voice services will have different characteristics. New services can support new features and new functionality with potentially better prices and more innovation.

8.47 The evolution of voice services lowers barriers to entry for the provision of primary fixed voice services and the cost of providing the service will fall to very low levels. We may see more companies enter, with better prices and more innovation; for example, intelligent call-blocking to combat nuisance calls, redirection and high-definition sound quality.

Disruption to consumers as a result of migration should be limited

8.48 It is important that migration itself does not cause disruption. Migration will work best where people migrate voluntarily, and where providers' migration strategies rely on developing new services which make it attractive to move.

8.49 For many, migration to voice over IP will be voluntary. For those who have and use a fixed telephone line within the home, PSTN migration should result in little noticeable change, both in terms of the consumer experience, and of the steps required to make the change. For consumers who already use a broadband connection for data services, it should be a relatively simple matter of moving their existing telephones from the PSTN to their broadband connection, via an adapter or suitable broadband router.

Some consumers may face challenges during migration

8.50 Whilst PSTN switch off should have few implications for most consumers, for others there may be important challenges which require careful consideration.

8.51 There are 1.5m landline-only consumers in the UK. For these customers, broadband technology will need to be installed in the home in order for fixed telephony services to continue. While this technology may be capable of supporting telephony and broadband, it may have only the telephony elements of the service activated, depending on customer

[106] Single Order Generic Ethernet Access – see https://www.openreach.co.uk/orpg/home/products/superfastfibreaccess/fibretothecabinet/fttc.do

[107] https://www.ispreview.co.uk/index.php/2017/07/openreach-extend-phase-2-trial-sogea-standalone-fttc-broadband.html

requirements and demands. Alternatively, customers who want voice-only services may be offered a telephony-only router. Where required, voice services can be delivered to consumers in a manner that looks like traditional telephony, and consumers may not be aware that the underlying connection is now broadband.

8.52 Customers with mobility, visual or other vulnerabilities may need assistance in installing the new equipment even if they only expect to use the new technology for voice services.

Compatibility issues for applications currently using PSTN signalling

8.53 There are a number of applications and services which currently run over the PSTN and its associated analogue access network which depend on technical characteristics of these networks and platforms beyond the basic delivery of voice, such as way that the PSTN handles signalling and other "in band" tones in and between networks. These include fax machines and dial-up modems (for point of sale card readers for example) as well as point to point connections for industrial purposes such as process monitoring.

8.54 PSTN switch off also raises concerns about other services which may be required in an emergency. Certain social care devices, such as personal alarms, have traditionally run over the PSTN. The calls that these devices make can traverse a number of different networks between source and destination, and as some of these intermediate networks migrate to IP-based technologies, interoperability issues are beginning to manifest.[108]

8.55 The scale of these problems may increase as widespread migration of networks from traditional to IP-based technologies increases. However, as network technologies are evolving, so too are the services and devices that run over them, in order to become more IP-compatible, and therefore able to offer additional functionality and features.

8.56 The providers of such services have already engaged with the Ofcom industry group established during 2017 and are liaising with providers regarding their migration plans and service compatibility issues, to ensure that services can remain operational or are superseded in good time before PSTN switch-off occurs.

8.57 As providers begin this migration, it is clear the process will need to take into account the needs of these specialist service providers and end users.

Consumer protection principles that Ofcom will apply during migration

8.58 It is important that we are satisfied that proposed migration processes will not result in harm or poor outcomes for consumers and businesses. Our aim is to ensure that migration does not result in undue disruption to customers, and that they are no worse off, either financially or functionally, as a result of it.

8.59 In last year's Connected Nations, we set out the principles we would apply during migration to achieve this aim. These will continue to underpin our approach:

[108] See p10-12 https://www.tsa-voice.org.uk/sites/default/files/TSA301664%20Whitepaper_Oct17%20120917_ONLINE%20VERSION%20ONLY_0.pdf

- Emergency services access should be provided in accordance with the General Conditions (GCs). The GCs have recently been revised; the revised provisions will come into force from 1 October 2018. They include GC A3 on the Availability of Services, including access to emergency services and a new provision (GC C5.2) for Regulated Providers to establish, publish and comply with clear and effective policies and procedures for the fair and appropriate treatment of consumers whose circumstances may make them vulnerable.
- Technical solutions for ensuring reliable operation of new voice services, for example during localised or widespread power outages, should provide levels of protections equivalent to that provided by traditional means. We will assess the suitability of such solutions on a case-by-case basis, taking into account the technical limitations and customer usage of both the traditional and new services.
- New voice services will maintain existing protections for vulnerable consumers in a manner which is appropriate for the technology they employ and their usage.
- Equivalents to the current social phone tariffs will be applied to future voice services where appropriate.
- Before and during any planned withdrawal, providers of existing voice services will work with third party service providers which rely on them, in order to minimise end customer disruption. In particular, voice service providers should make all reasonable efforts to ensure their changes do not cause excessive disruption to services used by vulnerable customers, such as personal alarm systems.
- Providers of traditional voice networks must give reasonable notice to their wholesale customers of any intention to withdraw relevant voice services, or to replace them with alternatives based on different network technology.
- Customers who do not migrate on a voluntary basis should be no worse off than they were before migration.
- Vulnerable consumers must receive any assistance they require for the migration process and continue to receive a service they recognise as a telephony service.

8.60 In order to assess how providers' migrations plans meet these principles, we are engaging with providers to understand their planned approaches. In particular we are seeking to understand:

- The timing and form of their migration process both for customers who move voluntarily, and those who do not;
- Their plans for communicating the changes and implication to end users;
- How they plan to identify and respond to the needs of vulnerable consumers;
- The implications for regulated services such as text relay, public call boxes and social tariffs;
- The pricing of the replacement services in particular to ensure that voice only customers are not worse off as a result of moving to VoIP;
- How they will ensure the emergency access requirements for free access, caller location and prioritisation apply to their new services;
- Their plans to ensure uninterrupted access to the emergency services in the event of local power outages;

- The general level of resilience of the replacement services;
- Their plans for liaising with third party providers such as telecare provers and for making their customers aware of the implication of the changes for those services.

Ofcom is working with industry to prepare for PSTN switch off

8.61 As part of the PSTN migration to an All-IP solution, we have commissioned the NICC[109] to develop new and update existing standards to support the new All-IP voice network and access environment.

8.62 A task group has been formed by NICC comprising experts from across the industry to define the standards for Voice over Broadband (VoBB) and consider how Voice band data should be carried over an All-IP network. This All IP Task Group is updating industry guidelines, with the aim of writing equivalent standards for the new All-IP voice service. Specifically, the standards under review are:

- ND1431 – Guidance on CPE Compatibility on NGNs and NGAs
- ND1443 – Guidelines for the Security of All-IP Service in the UK Telecommunications Network
- ND1704 – End to End Network Performance Rules and Objectives for the Interconnect of NGNs

8.63 These standards should provide clarity and consistency not only to UK communications providers for network interconnect purposes, but also to service providers in assessing the risks to existing services. The production of standards also helps provide a common baseline for the testing of services in the future.

8.64 We welcome the progress that has been made in this area over the past year and the continued engagement of major providers. We also note that the NICC has invited many of the relevant trade associations to the task group sessions to allow direct technical dialogue between the communications providers and service providers such as those associated with security and telecare alarms and point of sale terminals. This has led to a greater appreciation of the challenges and scale of the migration required for non-voice devices and has also helped the understanding of issues currently arising as a result of interworking between newer IP and legacy PSTN core networks. Ofcom and industry anticipate many of these issues will be resolved as the entire end to end path migrates to All-IP, leading to the elimination of PSTN/IP interconnect points. In the meantime, we will continue to help the dialogue between the various organisations involved to identify and address issues as they arise.

8.65 While the responsibility to ensure that migration does not result in disruption to end users lies with industry, we recognise the role Ofcom can play in setting out expectations for switch off and maintaining oversight of its implementation by industry. Since the publication of last year's Connected Nations report, we have set up an inclusive cross

[109] NICC is the technical forum for the UK communications sector agreeing interoperability standards for public communications networks and services.

industry All-IP Forum chaired and facilitated by Ofcom at which plans for migration and known or potential issues can be discussed. This group is attended by both communication providers and organisations representing service providers that may be particularly at risk as a result of migration, and helps industry develop improved communication and working practices. We expect these meetings to continue as individual providers adapt their migration timescales and as new challenges are identified and resolved. To support this activity we have further commissioned the NICC All IP Task Group to develop a test case document outlining how testing between communications providers and service providers should be conducted, this document is due for publication early 2018.

8.66 In the coming year we expect continued activity in the above areas with Ofcom continuing its oversight and facilitation role to help identify services and consumers affected and ensure communications providers establish effective plans to migrate consumers with minimum disruption and with vulnerable consumers protected.

8.67 In order to ensure that appropriate action is taken by relevant public sector stakeholders, we are also initiating a contact programme with lead Government departments and other agencies with responsibility for key sectors and policy areas.