Section 8

Security and resilience

Overview

8.1 As we increase our dependence on the nation's communications infrastructure, the security and resilience of fixed, mobile and broadcast television networks and services become ever more important. This section summarises the major security and resilience issues that were reported to Ofcom over the past year.

8.2 Important points to note are:

8.2.1 The majority of security incidents reported relate to **voice services**, often affecting consumer access to the 999 emergency services;

8.2.2 The majority of incidents are caused by the **failure of hardware components, the loss of power supply or by software bugs**; and

8.2.3 Incidents with an impact above one million customer-hours are uncommon, and are often the result of a **unique and unexpected threat to security**.

Our role in security and resilience

Ofcom and providers of communications networks and services are subject to certain requirements[73]. 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 Ofcom.

We first published guidance on the full range of security requirements in May 2011 and updated that guidance in August 2014.[74] 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[75] to meet high standards of reliability and to provide us with an annual report on transmission performance.

[73] In accordance with Article 13a of the Framework Directive[73], sections 105A-D of the Communications Act 2003 place requirements on providers and Ofcom regarding the security and resilience of communications networks and services.
[74] http://stakeholders.ofcom.org.uk/binaries/telecoms/policy/security-resilience/ofcom-guidance.pdf
[75] http://stakeholders.ofcom.org.uk/binaries/broadcast/guidance/techguidance/tv_tech_platform_code.pdf

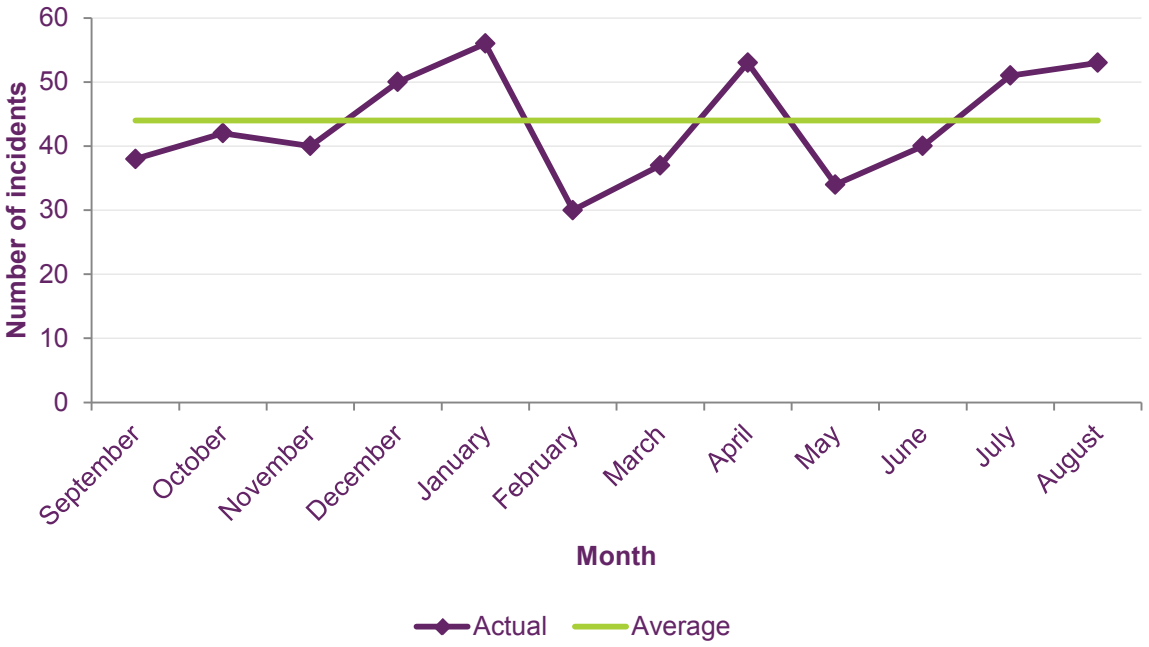
Resilience of fixed and mobile networks

The majority of security incidents reported relate to voice services, often affecting consumer access to the 999 emergency services

8.3 In the past year, 524 security incidents were reported to us by fixed and mobile providers. The vast majority of 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 2014 and August 2015. The monthly variation can be as great as 30% of the average and could be the result of seasonal factors such as weather or school holidays. We continue to monitor for trends over time.

Figure 38: The number of incidents reported between September 2014 and August 2015



Source: Ofcom analysis of operator data

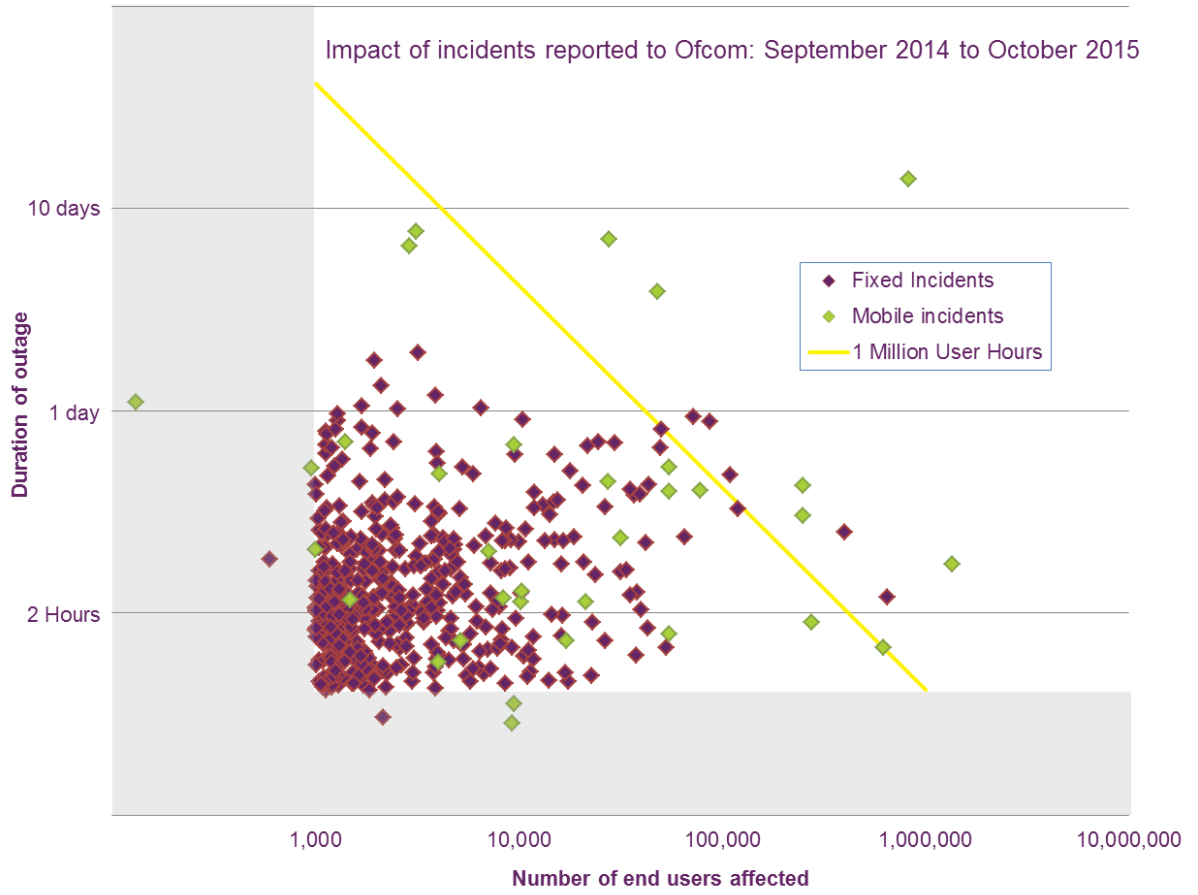
Scope of Ofcom reporting guidance/ framework

8.5 Ofcom's 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. Figure 39 shows the customer-hours impact of the 524 incidents reported to Ofcom.

Figure 39: The impact of incidents reported to Ofcom, between September 2014 and October 2015



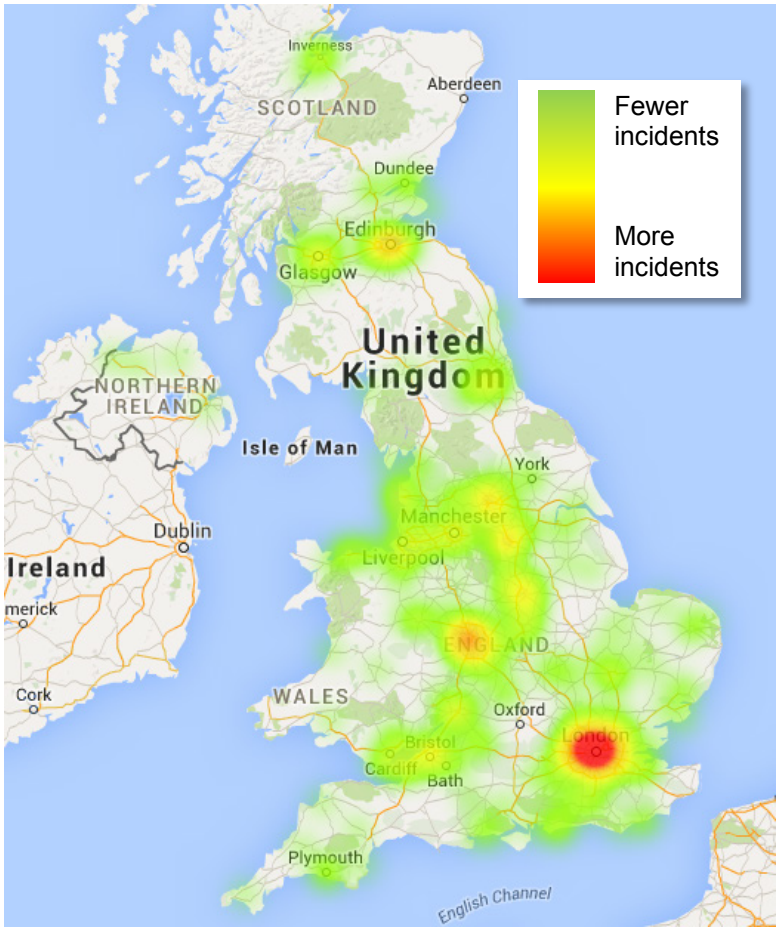
Source: Ofcom analysis of operator data

8.7 The majority of incidents have a relatively low customer-hours impact and are reported under the 'emergency services access' threshold.

8.8 Of the 524 reported incidents, 486 affected fixed networks and 38 affected mobile. The difference between these figures is explained by the emergency roaming agreement in place between mobile operators. This means that mobile operators have significant resilience in place for emergency service availability and therefore do not report often under the 'emergency services access' threshold.

8.9 Our revised 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. The number of mobile incidents reported to Ofcom is more than double that of last year.

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



Source: Ofcom analysis of operator data

8.10 Figure 40 shows how the 524 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.

8.11 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.

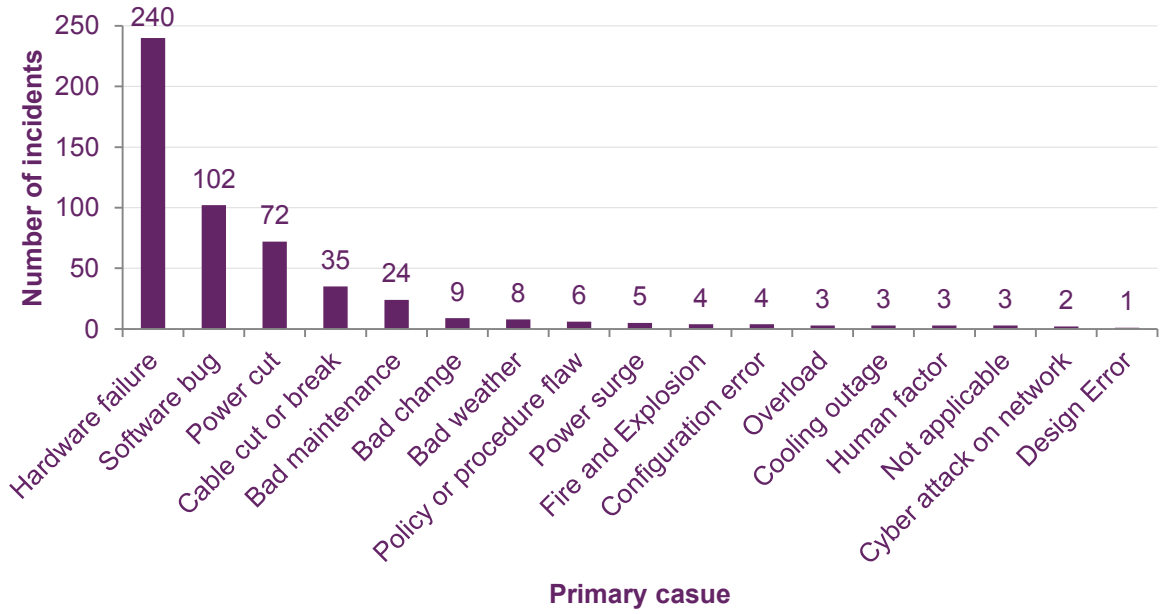
The majority of incidents are caused by the failure of hardware components, the loss of power supply or by software bugs

8.12 Establishing the root causes of incidents is central to understanding risks to the security and resilience of networks and services. System failure is overwhelmingly the root cause of significant network incidents; for the third year in a row over 95% of reported incidents fall into this category. This includes hardware and software failures, and the failure of systems, processes and procedures.

8.13 The remaining categories are human error, natural phenomena (which includes severe weather) and malicious actions, which were responsible for 3%, 1% and <1% of the reported incidents, respectively.

8.14 Figure 41 shows that incidents were reported against a wide range of primary causes[76]. 'Hardware failure' is the most common primary cause, followed by 'software bug' and 'power cut'. Together these causes account for over 75% of the incidents that are reported to us.

Figure 41: Primary cause of incidents reported to Ofcom, September 2014 to August 2015



Source: Ofcom analysis of operator data

Incidents with an impact above one million customer-hours are uncommon, and are often the result of a unique and unexpected threat to security

8.15 The European Union Agency for Network and Information Security (ENISA) is a centre of network and security expertise for the EU. ENISA provides guidance[77] on the reporting of security incidents. This includes the requirement for national regulatory authorities, such as Ofcom, to report annually on incidents with a significant impact; this is defined as those incidents with an impact above one million customer hours.

8.16 In the reporting period of September 2014 to August 2015 there were 12 incidents which met this threshold: seven affected mobile networks and five affected fixed networks. System failure is still the main root cause, at 75%.

[76] 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

[77] ENISA Technical Guidance on Incident Reporting. https://resilience.enisa.europa.eu/article-13/guideline-for-incidentreporting/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf

Cyber security

8.17 Security incidents in the communications sector do not always affect the availability of networks and services. Communications providers can and will be subject to cyber-attack, which is increasingly common across all industries. These attacks are often related to the theft of data or intellectual property, but do not affect the operation of the network or service directly.

8.18 Two recent examples are the widely-reported cyber-attacks on TalkTalk[78] and Vodafone[79]. In both cases hackers attempted to access customers' private information, with varying degrees of success. In such circumstances Ofcom collaborates with the communications provider, the Information Commissioner's Office (ICO) and the appropriate Government departments (particularly DCMS) and agencies, to ensure that the risks to the consumers of communications services are being addressed. The ICO is the primary regulator on data protection issues, so compliance with data protection law, and the investigation and possible sanctioning of data security, such as the data breach of TalkTalk's website, is first and foremost a matter for the ICO80. In parallel, law enforcement agencies have responsibility for investigating any criminal aspects of the cyber-attack that led to the data breach.

8.19 The Centre for the Protection of National Infrastructure (CPNI) protects national security by providing protective security advice. Protective security is "putting in place, or building into design, security measures or protocols such that threats may be deterred, detected, or the consequences of an attack minimised". It provides advice on physical security, personnel security and cyber-security/ information assurance. The CPNI operates a number of 'Information Exchanges' which facilitate the exchange of information, advice and guidance between its members, the providers of different aspects of the national infrastructure, which includes the UK electronic communications infrastructure.

8.20 CESG, the Information Security arm of GCHQ, is the National Technical Authority for Information Assurance within the UK. It builds national capability through the provision of standards and guidance, working with industry to ensure that appropriately assured products, services and people are available, and building up a pool of world-class information assurance and cyber-security professionals on whom organisations can draw. Its role includes working with industry to protect the Critical National Infrastructure of the UK.

8.21 CERT-UK is the UK National Computer Emergency Response Team, formed in March 2014 in response to the National Cyber Security Strategy. It has four main roles:

- national cyber-security incident management;

[78] http://www.talktalkgroup.com/press/press-releases/2015/cyber-attack-update-november-06-2015.aspx
[79] http://mediacentre.vodafone.co.uk/pressrelease/statement-on-unauthorised-account-access/
[80] The ICO enforces two pieces of separate legislation dealing specifically with protecting the confidentiality of data, including personal data, associated with the network or service: the Data Protection Act 1998 (http://www.legislation.gov.uk/ukpga/1998/29/contents) and the Privacy and Electronic Communications Regulations 2003 (http://www.legislation.gov.uk/uksi/2003/2426/regulation/22/made).

- supporting critical national infrastructure companies in their handling of cyber-security incidents, This includes the Cyber Information Sharing Partnership (CISP) which enables companies to share what they know;

- promoting cyber-security situational awareness across industry, academia and the public sector; and

- providing a single international point of contact for co-ordination and collaboration between national CERTs.

8.22 On 17 November 2015, the Chancellor of the Exchequer announced that these structures and bodies would be reformed, with the establishment in 2016 of a new National Cyber Centre, which will report to the Director of GCHQ, and which will take over some or all of the responsibilities of the existing bodies. Consequently, the way in which Ofcom works with other agencies may change in the future to ensure that we continue to collaborate effectively.

8.23 Although cyber security is not referenced in current underpinning legislation, the existing Ofcom guidance on network security and resilience does address the issue specifically, setting the expectation that providers will take appropriate steps to manage the cyber threat and take account of relevant Government advice such as the "10 Steps to cyber security[81]" and the Cyber Essentials Scheme[82]. We have recently written to the largest providers within the sector, reminding them of this guidance and seeking assurance that they are following it.

[81] https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary
[82] https://www.gov.uk/government/publications/cyber-essentials-scheme-overview