Hutchison 3G UK Limited’s response to Ofcom’s Review of Security Guidance

7 September 2017

Three.co.uk

Introduction

1 This is Three's (Hutchison 3G UK Ltd) response (the "**Response**") to Ofcom's consultation on updating Ofcom's guidance on security requirements in sections 105A to D of the Communications Act 2003 (the "**Consultation**").

2 Three welcomes Ofcom's decision to update its security requirements guidance. Given the dynamic nature of technology and telecoms markets this guidance needs to be regularly refreshed to remain relevant and, crucially, to provide greater legal certainty to communications providers ("**CPs**") in this area. Three also considers that clearer and more detailed guidance is needed to ensure operators gain a better understanding of Ofcom's expectations from a compliance perspective in this area e.g., Ofcom needs to set out with practical examples the "appropriate measures" and "documentary evidence" Ofcom typically expects to see.

3 While Ofcom's decision to update its guidance is welcomed, Three is concerned by a number of the changes proposed by Ofcom.

4 The following response is made up of some general comments on the approach adopted by Ofcom in its Consultation, followed by specific comments on the principal issues addressed by Ofcom in its Consultation.

General comments:

Significant increase in the burden upon CPs

5 Three is particularly concerned that some of the changes are disproportionate and significantly underestimate the increased burden to implement these proposals. Specifically, these are in relation to:

- *Incident reporting*: while Three welcomes Ofcom's proposal to achieve greater clarity by revising the mobile reporting thresholds, Three is concerned by the proposed new thresholds. Significant operational resources will be required for CPs to comply with the new reporting thresholds and urgent incident reporting criteria on an ongoing basis. The proposed regime would be extremely burdensome for Three and other operators; particularly during live incident management when CPs' incident management teams are focussing on remediation activities. Furthermore for the reasons set out in paragraph 30 *et seq*. of the Response, Three does not consider that the significant increase in costs for CPs will lead to a corresponding increase in the efficacy of the reporting regime.

- *Power and flood resilience*: as implementing increased power and flood resilience represents a significant expense for operators, greater clarity from Ofcom is required on the proportionality assessment that CPs are expected to conduct in assessing whether such measures are necessary.
- *Auditing*: the increased use of Ofcom's audit powers under s105(C) will have direct cost and resource implications for CPs.

Further clarity is required from Ofcom before Three can meaningfully comment on certain of the Consultation's proposals

6 Three notes that Ofcom has not provided a proposed revised draft of the security requirements guidance for comment as part of the Consultation. As a result, Three is concerned that, in a number of instances, insufficient information is provided in the Consultation to enable Three to understand how the proposed changes will operate in practice and meaningfully comment on the approach adopted by Ofcom.

7 Some examples of this are set out below:

- *Cyber vulnerability testing*: although, in principle, cyber vulnerability testing could be a useful educational tool for CPs, Ofcom should provide greater clarity on how a telco equivalent of CBEST would operate in practice.
- *Power resilience*: the Consultation provides at paragraph 2.35 that Ofcom will reflect "*an increased focus on this issue in our revised guidance*." The Consultation does not clarify, however, how Ofcom intends to amend the existing guidance and whether it anticipates any significant change to the existing obligations imposed on telecoms providers.
- *Auditing*: Ofcom notes at paragraph 4.7 that: "*we propose to change the current guidance to reflect that we may consider exercising the power to conduct audits more often than previously*." Prior to increasing the use of Ofcom's audit powers, however, Three considers that Ofcom should ensure that clear safeguards are in place to ensure that these powers are used in a fair, transparent and accountable manner. It would also be helpful to have some more practical examples of when Ofcom considers it would be necessary for Ofcom to exercise such powers.

Summary of Response

Security and Availability (s105A)

Cyber security

8 Three recognises the central importance of cyber security to telecoms networks and welcomes Ofcom's focus on this area. In addition, Three supports Ofcom's position that it may be disproportionate to expect large CPs to strictly comply with third party accreditation schemes (e.g. Cyber Essentials Plus).

9 Three is particularly concerned by the more onerous and impractical requirements of complying with certain elements of the Cyber Essentials Plus. As Ofcom recognises at paragraph 2.15, the Cyber Essentials Scheme was designed for smaller organisations and it would not be appropriate or proportionate for large MNOs with complex IT systems to comply (without significantly altering the scope of the Cyber Essentials).

In this context, Three is also concerned by Ofcom's suggestion (at paragraph 4.11 of the Consultation) that it may audit compliance with provisions in the Cyber Essentials Scheme requiring the application of security patches within 14 days of becoming available to protect a CPs' internet connected desktop PCs. [✂] Three therefore asks Ofcom to work with CPs on such requirements before implementation to ensure their practical applicability.

10 Similarly, although Three agrees that CPs should have regard to the guidance issued by that National Cyber Security Centre (NCSC); it would not always be reasonable (or indeed possible) for CPs to implement NCSC recommendations in full (particularly where there are dependencies on third parties, such as device manufacturers). [✂]

11 Finally, given Ofcom's consultation appears to indicate a heightened monitoring and enforcement of telecoms providers' cyber and data security systems, Three requests that Ofcom clarify what it regards as the delineation of responsibilities between the ICO and Ofcom with respect to enforcement action.

Minimum Security Standard for Interconnection – NICC ND1643

12 Three agrees with Ofcom's comment at paragraph 2.18 that "*the continued lack of universal adoption of [the ND1643] standard undermines the effectiveness of the measures taken by those which have adopted it*" and notes Ofcom's comment that "…*there are no checks to ensure all companies doing so are interpreting the standard*

consistently. This potentially undermines the value of the certificates." In Three's view, reform in this area is welcome as parts of the current standard are ambiguous and improvements can be made.

13 Given the ambiguity of the current standard, Three also agrees with Ofcom that it would be helpful to have a contemporary "*minimum security standard for interconnection*" that makes clear to CPs what is practically required by the NICC's new "*best practice*" document and that measures are feasible in practice.

Cyber vulnerability testing

14 Three understands DCMS plans to introduce a telco equivalent of CBEST. Three would be happy to work with Ofcom on the DCMS telecoms scheme.

15 Three's understanding of CBEST testing in the financial sector is that it is a voluntary scheme which primarily serves an educational function to incentivise compliance; allowing financial institutions to test and improve their resilience to cyber security threats and regulators to understand associated risks. It is not intended to form a basis for enforcement action and has not done so to date.

16 In principle, Three considers that cyber vulnerability testing under a new telco scheme could be a useful educational tool for MNOs to test and improve their resilience to cyber security threats, and help regulators to understand associated cyber risks. However, Three would need greater clarity on how a telco equivalent of CBEST would operate in practice in order to comment meaningfully on the proposals in the Consultation.

17 Furthermore, as such additional testing would place significant burdens on operators, Three would be keen to participate in the design phase of the scheme to ensure the requirements are practical and workable for CPs. Indeed, Three notes in this respect that the IT systems used by telecoms providers are significantly more complicated than those used by banks.

Maintaining network availability

Single points of failure

18 Three notes Ofcom's increased enforcement activity in relation to single points of failure and considers that CPs would benefit from much greater clarity on Ofcom's expectations in this area.

19 At paragraph 2.30 of the Consultation Ofcom helpfully clarifies that it considers that "*avoiding single points of failure, where it is reasonably possible to do so, is likely to be an "appropriate step" within the meaning of s105A (4).*" In Three's view, more detailed, clearer guidance is needed, with practical examples of what Ofcom would consider "reasonably possible" in this context. As network design is a complex matter, CPs need sufficient certainty on where the boundaries fall in this area to help them make network design decisions with greater [✂] legal certainty.

20 Three welcomes Ofcom's clarity at paragraph 2.30 of the Consultation on the relevant considerations Ofcom will take into account but believes it does not go far enough. More detailed guidance is needed, for example:

- Ofcom points out that one relevant consideration is "*it is more likely to be disproportionate to deploy protection paths in the access network than in a CP's backhaul and core networks.*" This comment only assists CPs to a limited extent as Ofcom has not clarified what it means by "backhaul" in this context. Backhaul can be used at various parts of a CP's network, for instance backhaul can be used [✂]. Technical definitions need to be clear given complexities in network design.

- Ofcom confirms that, where there is only a certain number of customers relying on the single point of failure, it is reasonable for operators to e.g. include a single point of handover or interconnection for traffic. Could Ofcom please provide further clarity by reference to an approximate number of customers?

- What does Ofcom mean by geographic and physical constraints?

- What standard does Ofcom expect for data centre resilience? CPs need to know this when setting SLAs for third parties they work with.

- What does Ofcom consider a reasonable cost in terms of expenditure to secure resilience in this area? And does this cost burden vary depending on the size of the operator?

- Does the standard differ for emergency and non-emergency traffic?

- What happens if a customer can switch between different technologies and/or roam on to another network?

21 On Ofcom's comments at paragraph 2.31 of the Consultation, it would also be helpful if Ofcom could clarify (with examples) what evidence Ofcom is looking for to show that "*the CP has assessed the risk involved in their network design choices, and has met their obligations to take all appropriate steps to protect availability*."

Flood resilience

22 Ofcom is proposing to update guidance to reflect the growing risk to the availability of service from flooding in line with Government policy. [✂]. Three cautions that Ofcom must take a proportionate approach to guidance on flood resilience, including the time that it takes to upgrade sites and to acquire the appropriate rights to do so.

23 Additionally, Ofcom guidance must recognise that flood resilience is often costly and the risk of flooding although serious is often very low. It is also imperative that Ofcom take account of overlapping coverage across cell sites which may mitigate the risk of network availability caused by flooding at a single cell site.

Outsourcing

24 Three welcomes Ofcom's comment at paragraph 2.37 of the Consultation on its expectations where network functions are outsourced and notes that it accords with the steps that Three already undertakes to ensure appropriate governance of outsourced functions. Three does, however, note that Ofcom's proposals are limited to contractual controls over third parties. Three notes that in other regulatory regimes (e.g., GDPR) third parties bear joint liability with networks for ensuring compliance with regulatory obligations (see Article 28 of GDPR). Three considers that, in order to incentivise third parties to ensure full compliance, it would be helpful if Ofcom could also consider and clarify when it will use its enforcement powers in relation to third parties where appropriate.

Incident Reporting (s105B)

25 Three supports Ofcom’s proposal to introduce clearer guidance in this area. However, Three’s overarching concern with the proposed mobile reporting thresholds is that they will lead to a significant increase in the number of reportable incidents which are not service impacting and crucially have no impact on the availability of emergency services. For the reasons explained below, this approach is disproportionate and significantly underestimates the operational resources required for MNOs to comply. Furthermore, [✂]. Three hours is an exceptionally short timeframe for reporting (particularly outside of normal business hours), [✂].

26 In Three’s view, the proposed regime will be extremely burdensome for Three and other operators, would lead to [✂]without a corresponding increase in the efficacy of the reporting regime, and that the regime could be particularly burdensome during live incident management when CPs’ incident management teams are focussing on remediation activities.

27 [✂].

28 Three would like the opportunity to work actively with Ofcom and the other MNOs to define mobile reporting thresholds that can achieve Ofcom’s objectives, while minimising the adverse impact on MNOs. We believe this would enable Ofcom to develop effective and proportionate reporting criteria.

Mobile reporting thresholds

29 Ofcom notes at paragraph 3.15 of the Consultation that its objective is “*to receive a significant and sustained increase in reporting from those MNOs which are currently reported infrequently, while avoiding a reporting process which is unduly burdensome*.” Three anticipates, however, that the mobile reporting thresholds proposed in the Consultation will result in a significant burden on MNOs caused by the increase in the number of notifications that will be required, many of which are likely to be about incidents that are non-service impacting with no adverse impact on customers. In particular, Three has the following concerns:

- Ofcom’s proposal to cover a very wide definition of “*service loss or major disruption to voice and/or data services for one or more technology from 25 or more sites*” in its reporting criteria at paragraph 3.18 of the Consultation will [✂].

- In Three's view, this is too wide a definition and a more proportionate approach needs to be applied by Ofcom on which incidents they are targeting. Practical examples of the type of incidents this aims to capture would also be a welcome addition. This wide definition risks an unduly burdensome regime requiring reports that would have no adverse impact on customers. It would also be helpful if Ofcom could clarify, with practical examples, what it means by "major disruption" so CPs are clear on the type of incident to be covered.

- It is also not clear why Ofcom requires a notification to be made in instances where only one technology has been impacted by a network incident, given that there may be no customer impact. In Three's view, this point should be reconsidered and explained further.

- Three also has significant concerns about the numerical reporting criteria for rural areas. Three considers that imposing a reporting requirement with respect to single site issues [✂]. Three is concerned that this requirement is unduly burdensome given that it is possible CPs [✂] but would nevertheless meet the proposed reporting thresholds.

Calculating the number of users affected

30 Three welcomes Ofcom's clarification that it will not require detailed estimates of the number of customers impacted by an incident until some time after the incident has been resolved. However, estimating the number of customers impacted by a network incident [✂].

Reporting affected sites

31 Three recognises Ofcom's desire to understand the geographic impact of mobile incidents. Given that the mobile reporting thresholds proposed in the Consultation will likely [✂], however, Three notes that providing a full list of affected sites for all reportable incidents will further increase the volume of data required to be notified to Ofcom (and hence the burden on CPs).

Cyber incident reporting

32 Three understands that Ofcom is seeking to update its guidance to clarify that cyber incidents with a significant impact on the operation of a CP's network or services are reportable.

33 Three considers that it would be helpful for Ofcom to clarify:

- That cyber incidents solely impacting a CP's "corporate" systems, with no impact on consumer-facing activities (for example [✂]), would not be reportable under s105B.
- In cases involving data protection/security incidents, how Ofcom proposes to work with the ICO to avoid duplicative investigations into the same incident (which would be disproportionate and impose an unnecessary burden on CPs).

24/7 reporting process for urgent incidents and subsequent changes to other reporting timescales

34 Three strongly opposes Ofcom's proposal to introduce urgent incident reporting criteria. As previously flagged to Ofcom**,** Three considers that an urgent reporting regime is wholly disproportionate and will impose a significant burden on incident management processes [✂], and divert critical resources away from resolving live incidents.

35 Three hours is an exceptionally short timeframe for the reporting of such incidents [✂].

36 This is particularly relevant where an incident occurs outside of normal business hours (e.g. on the weekend / early hours of the morning etc.)

37 Three also notes that the requirement to report cyber incidents within 3 hours is significantly more onerous than the UK Government's expected implementation of the NIS Directive, which proposes a requirement on "operators of essential services" in the UK to report cyber incidents: "*without undue delay and as soon as possible, at a maximum no later than 72 hours after having become aware of an incident*."[1]

38 Three is also concerned that several of the "urgent reporting criteria" proposed by Ofcom are not practical and will therefore be difficult to apply in practice:

- *Cyber attacks*: Ofcom itself recognises that assessing whether cyber-attacks meeting any of the qualitative criteria for reportable mobile incidents, can be a subjective and difficult exercise.
- *Incidents affecting services to 250k end users and expected to last 12 hours or more*: it is difficult in the initial stages of a network outage to determine whether an incident will last 12 hours or more.

[1] Section 7 of the DCMS Public Consultation on the Security of Network and Information Systems (August 2017): https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/636207/NIS_Directive_-_Public_Consultation__1_.pdf

- *Media coverage*: requires ongoing monitoring of media reports which is challenging in the context of an urgent incident occurring outside of regular business hours.

Audit & Enforcement (s105C & D)

39 Three acknowledges Ofcom’s powers to audit under s105(C). However, such powers must be exercised proportionately and with great care given the direct cost and resource implications for CPs. Three would welcome greater clarity on how Ofcom’s test for proportionality in this regard, setting out in particular how Ofcom will exercise these powers in a fair, transparent and accountable manner.