BT’s response to Ofcom’s consultation on its Review of Security Guidance

7 September 2017

Comments should be addressed to:
Alex Quinn, BT Group Regulatory Affairs, at C8, BT Centre, London, EC1A 7AJ
e-mail alex.quinn@bt.com

Contents

Executive Summary

1. This response sets out BT's thoughts on Ofcom's proposals in their Review of Security Guidance consultation document. Many of Ofcom's proposals are welcome as they provide more clarity and guidance with better defined expectations of CPs. However there are areas where Ofcom needs to reconsider their proposals and discuss further with CPs how their needs can be best met. In particular Ofcom's understanding of their role and remit with regards to cyber security incidents does not align with BT's interpretation of Section 105 and it is important that Ofcom takes this opportunity to work with CPs and other organisations to ensure a common understanding.

2. Furthermore Ofcom's proposals around urgent incident reporting could benefit from a more informal approach, and some of their criteria could be further defined to provide clarity around expectations. Ofcom also needs to ensure that its changes to mobile incident reporting are suitable and not excessively burdensome given the technological and reporting challenges that exist, and therefore will produce better outcomes than the current processes in place. We believe Ofcom could benefit from further discussion with mobile operators around this area.

Introduction

3. BT welcomes this opportunity to comment on Ofcom's consultation on its Review of its Security Guidance. BT agrees with Ofcom that networks are a critical part of the national infrastructure. Therefore it is vitally important that Ofcom's guidance reflects this criticality but also that it is clear with respect to the obligations that fall upon communications providers (CPs). It is also important that these obligations reflect a true assessment of the risks and costs involved if incidents do occur, and that Ofcom doesn't seek to impose excessive burdens on CPs when considered against the level of impact that may occur.

4. BT welcomes and supports Ofcom's intention to keep its guidance up to date in order to reflect the current environment as well as Ofcom's desire to clarify its expectations of CPs with regards to security and availability and incident reporting. Whilst BT welcomes many of Ofcom's proposals and suggestions in their document it also has serious concerns about some of them, in particular Ofcom's understanding of their role and remit with regards to cyber security incidents. It is vitally important that the responsibilities of Ofcom and other organisations, namely the ICO, are distinct and clear, and Ofcom's proposals risk blurring the lines. Ofcom should seek to avoid such confusion. We detail our objections to Ofcom unilaterally redefining their remit below and encourage Ofcom to engage with the current DCMS consultation to ensure that reporting lines are clearly defined across industry.

5. BT also believes that Ofcom formalising the urgent incident reporting process carries significant risks and could result in unintended negative consequences. Ofcom should consider how such guidance would work in practice and whether it can take a more informal approach that would better achieve its aims. We outline our concerns further when we discuss the urgent incident reporting process below.

Obligations under s105A

Cyber-security

6. BT takes the threat of all cyber-attacks seriously and understands the threat they pose to the security of public electronic communications networks and services. Where such cyber-attacks affect the functioning of the network or services then BT would consider that they fall under the remit of Section 105 and already abides by the guidance set out by Ofcom relating to Section 105b incident reporting.

7. BT recognises the pivotal role the NCSC now plays and we support Ofcom's proposals to utilise guidance and best practice from the NCSC as suggested in paragraph 1.4 of Ofcom's consultation document.

8. BT also understands the threat of cyber-attacks to data security and integrity and the risks they present. BT takes all of its information and data protection obligations seriously and follows reporting guidance laid out by the ICO.[1]

9. Ofcom however seems to conflate the threat of data integrity and security with the managing of risk and minimising impact of security incidents to the provision of public electronic communications network and services. BT does not believe that, serious though it may be, a data breach classifies as a failure of the network or of its services and therefore should not be included in any guidance under Section 105 given the wording and the intention of the Communications Act 2003:

10. *"105A.—(1) Network providers and service providers must take technical and organisational measures appropriately to manage risks to the security of* ***public electronic communications networks and public electronic communications services." [emphasis ours]***

11. This Section is clearly intended to refer to incidents that affect the network or service availability; a loss of personal data, whilst in itself a serious incident would unlikely do this. Therefore to incorporate such incidents under this guidance would be to misinterpret or misrepresent the Communications Act 2003, which Ofcom should seek to avoid.

12. Ofcom itself appeared to agree with this interpretation when it previously published guidance in August 2014[2], where it stated in paragraph 3.2:

13. *"We note that there is a potential overlap with the requirements to protect the confidentiality of personal data in the Privacy and Electronic Communications Regulations. We understand that matters falling specifically under those Regulations are for the Information Commissioner's Office to consider."*

14. Therefore given the obligations CPs already have with relation to the ICO, Ofcom imposing their own separate obligations is outside Ofcom's remit under Section 105 and will result in an extra burden on CPs, but more importantly it will confuse the reporting procedures.

[1] https://ico.org.uk/media/for-organisations/documents/1583/notification-of-pecr-security-breaches.pdf
[2] https://www.ofcom.org.uk/__data/assets/pdf_file/0021/51474/ofcom-guidance.pdf

15. The impact of Ofcom extending the interpretation of Section 105 will blur the lines between the remit of itself and the ICO and could lead to CPs failing to meet their obligations to one of the bodies if they aren't clear on where the remits lie.

16. It is also worth noting that the government (DCMS) is currently consulting on the Security of Network and Information Systems[3], the outcome of which is likely to impact the roles of both Ofcom and the ICO in this area. BT has no objections to reporting data security and integrity incidents to either the ICO or Ofcom in principle, but it is important that only one entity has formal responsibility and powers in any one area and that the dividing lines are clearly defined. Ofcom should co-ordinate with DCMS and ICO to determine agreed guidance that can be delivered to industry.

17. In the meantime BT does understand Ofcom's concerns around data privacy and is willing to discuss with Ofcom how we can satisfy their need to remain informed without having to redefine Section 105 of the Communications Act 2003, and avoiding any issues of confusion or creating an extra burden upon CPs.

Risk Management and Governance

18. BT has strong security risk management and governance in place for operational risk right through to Board level reporting. Our risk management approach has led to a multi-year investment programme that has adapted to the changing risk landscape. Approach to certification has to be driven by assurance and customer demands within CPs own environments.

Cyber Essentials Plus

19. BT is certified to Cyber Essentials Plus and actively maintains that certification. BT has advised its suppliers where they are part of the Government supply chain of the need for certification. Since the requirement for certification is from Government, BT believes it has discharged its responsibility in this respect and will continue to do so. We have no issues with Ofcom's proposed guidance.

Minimum Security Standard for Interconnection – NICC ND1643

20. BT is certified to ND1643. BT is aware of the ongoing NICC review of the standard and its effectiveness and has already been in discussion with OFCOM and DCMS about the value of the scheme, particularly given its lack of enforced adoption across the industry. We will continue to ensure that we fulfil our obligations to employ appropriate security measures regardless of the status of NICC ND1643, though we would appreciate clarity on expectations once the review is concluded.

Cyber vulnerability testing

21. [✂]. BT also carries out its own regular pen testing and red teaming on our critical infrastructure. Any industry approaches need to reflect the security risk position of a CP.

[3] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/636207/NIS_Directive_-_Public_Consultation__1_.pdf

Single points of failure/Flood and Power resilience/Outsourcing

22. BT agrees with Ofcom's intent on ensuring that reasonable precautions are taken which prevent incidents from occurring, whether it is avoiding single points of failure, preparing for flood risks or power failures or ensuring that third party infrastructure is sufficient and BT already takes these precautions where appropriate.

23. Ofcom must however always bear in mind that the precautions CPs take must be balanced against the economic cost of doing so. It is essential that providing services doesn't become economically unviable and Ofcom must be careful not to insist on unrealistic levels of protection such that the service doesn't become unaffordable for customers. We would also be concerned if Ofcom expected CPs to prevent failures relating to infrastructure that isn't under their control that might have a knock on effect to their infrastructure, for example flooding could damage a bridge that in turn could damage BT's infrastructure. Whilst we'll continue to work with appropriate entities to address these dependency issues, Ofcom should be conscious that CPs will not always be responsible for all incidents.

24. BT has well established processes in place for managing security risks of outsource providers and recognises that outsourcing to a third party does not excuse us from our obligations under Section 105A.

25. We look forward to seeing Ofcom's expectations with regards to these prevention measures and hope that they will seek feedback and discuss the details with industry before finalising them.

Incident Reporting

Mobile Reporting

26. Any change to the level of detail being sought by Ofcom in relation to information collection and incident reporting must be objectively justified and proportionate to avoid placing an undue burden on CPs and their commercial partners. Ofcom needs to understand that costs are incurred even when the smallest of changes are proposed because more than one party is usually involved.

27. Different levels of reporting and information sharing already takes place through Government committees, such as TISAC. Ofcom should avoid unnecessary duplication of effort, as well as the potential for confusion if multiple reporting structures are in place covering the same incidents. Ofcom must also ensure that commercially sensitive information is fully protected (e.g. from Freedom of information requests and requests under the Environmental Regulations) and only used by Ofcom for the purpose of reporting at an aggregated level to Government and EU regulatory bodies to avoid risk of disclosure.

28. Establishing numerical reporting thresholds for EE is complex due to the nature of a mobile network. It has been difficult to determine how many customers are attached to sites at a single point in time during an incident. In early 2016 EE began looking at ways to measure customer impact and a tool was developed that could provide an approximation of customers affected based on the thresholds agreed previously between EE and Ofcom. Where the incident is not attributed directly to impacted sites (e.g. a 4G data incident) the tool would not be useful and customer numbers need to be estimated by other means.

29. However, we have a system today that works relatively well and much resource has been invested in getting to this point. When EE was subjected to a section 105C audit by the Ofcom-commissioned auditor, Actica, in September 2016, the outcome was satisfactory and EE had met the standards for its incident management and change management processes and procedures. No follow-up investigation was initiated by Ofcom.

30. We have reviewed the changes being proposed by Ofcom in relation to mobile incident reporting thresholds and the impact on EE's existing processes and procedures.

    a) *Service loss or major disruption to voice and/or data services for one or more technology (i.e. 2G, 3G and/or 4G) from 25 or more sites lasting for two hours or more.*

    We suggest that Ofcom uses 30 sites instead of 25 as the threshold for a P1 incident which falls in line with EE's existing reporting thresholds. [✂]

    [✂] Although EE welcomes the clarification for incidents greater than two hours (with caveats), we believe that the single site outages impacting one or more technologies will significantly increase the number of incidents reported to Ofcom. [✂] . We therefore propose that Ofcom either increases the time threshold by four or eight hours, and/or apply the time threshold only where multiple technologies are impacted by the incident, for example, an incident impacting 2G, 3G, and 4G.

    b) *Mobile voice or data service/network offered to retail customers in rural areas lasting 8 hours or more.*

    The EE network does not record configuration information within incident management systems that will enable the single site outages to be readily categorised as rural or urban. [✂]

31. Following discussions with Ofcom about customer impact assessment, we have determined that changes to the tool currently used to determine customers impacted by incidents will be necessary in line with Ofcom's proposals, should Ofcom be minded to make the proposed changes.

Cyber incident reporting

32. Cyber incidents should be reported to Ofcom under Section 105B when they have a *significant impact on the operation of a public electronic communications network or service*. Cyber incidents that do not meet this criteria do not fall within Ofcom's remit and it is important that we do not introduce complexity by having multiple reporting structures for such incidents. Given the current DCMS consultation (as referred to in paragraph 14 of this response), this provides an opportunity for all parties to work together to provide one simple reporting structure with clearly defined guidance, criteria and responsibilities. BT would encourage Ofcom to work with the ICO and DCMS in doing so in order to avoid confusion.

33. Until such a structure is defined BT will continue to fulfil its reporting obligations to the ICO. Given Ofcom cannot unilaterally expand the remit of Section 105B reporting obligations, BT could provide information relating to other reporting obligations to Ofcom on an informal basis where possible and would be happy to discuss how we might go about this. This would assist

Ofcom in understanding the nature and extent of cyber incidents without placing undue burdens on CPs, such as duplicative reporting obligations.

Reporting cycle

34. [✂]

Urgent incident reporting process

35. BT welcomes Ofcom's invitation to comment further on the "Serious/Urgent" incident reporting requirement first shared in its December 2015 letter to industry and as discussed during our January 2016 meeting and subsequent letter. During this meeting BT agreed to informally provide notification of urgent incidents to Ofcom.

36. It is not always possible to identify the scale of an incident early in the process nor is it sometimes possible to easily identify the "start point" of such incidents. Irrespective of these circumstances, BT has in advance of legislative drivers and Ofcom 24/7/365 reporting contacts being in place, worked to notify Ofcom of serious incidents which it believes meet the proposed enhanced incident reporting criteria as soon as possible after we have become aware.

37. Notification of such incidents has taken place utilising existing Ofcom contacts in the absence of contact information for a staffed Ofcom 24/7 reporting point which BT believed was imminent.

38. For clarity BT is happy to continue following this process, where we believe an incident is serious enough (i.e. we believe it would fulfil Ofcom's urgent incident reporting criteria), by providing details to Ofcom informally as soon as possible after becoming aware of the incident.

39. Though Ofcom should ensure the reporting point is staffed to receive such calls on a 24/7 basis in order to provide value to the process. Urgent reporting to a message service would not add sufficient value to justify this continued level of enhanced reporting moving forward, whether formal or informal.

40. However BT does not believe that it is appropriate for Ofcom to legislate within its guidance a formal process that CPs must follow relating to such incidents for the following reasons:

    a. During such incidents it is vital that the CPs attention is focused on restoring the network as soon as possible and the teams should not be distracted by considering the consequences of failing to abide by reporting criteria.

    b. As incidents develop the information about them will change quickly, therefore Ofcom shouldn't prescribe what CPs should report and when, and should leave it up to the CP to provide updates as appropriate when it gathers new information.

    c. Any information that is provided by CPs during this time will only be based on early indicators and is likely to be incomplete or possibly inaccurate. Ofcom should treat all information during this period with caution and therefore it is most appropriate to provide it informally. A formal process would imply the risk of sanctions for non-compliance or incorrect information. Therefore CPs would consider these risks and could actually be less likely to report information to Ofcom if they couldn't do so with certainty as to its accuracy. CPs would also likely put in place sign off processes

and checks to ensure that information provided to Ofcom under a formal process was complete and accurate and this would delay information provision to Ofcom.

41. If Ofcom includes the enhanced urgent incident reporting process within its guidance then it should be explicit that such guidance is a request to follow best practice and not a formal obligation and that CPs would not face sanctions when failing to report accurate information within such a short timescale in order to avoid the risks detailed above.

42. Secondly whilst BT acknowledges that Ofcom has stated reporting should be, wherever possible within three hours of the CP becoming aware, it would be helpful if Ofcom altered the guidance to specify that the three hour is the time from which point the reporting team within the CP becomes aware of it as suggested in our meeting of 14 January 2016. This will allow reporting teams to do appropriate investigations and checks on the information they receive about an incident prior to speaking to Ofcom if they do not become aware of it immediately. Otherwise it is likely that reporting teams may become aware of an incident close to or after the 3 hour deadline and in their rush to report to Ofcom may not provide relevant, useful or accurate information.

Urgent incident criteria

43. In addition to our objections above to Ofcom formalising the reporting process, BT also has some concerns around the criteria Ofcom has laid out.

44. Ofcom includes the criteria of “Incidents affecting services to 250k end users and expected to last 12 hours or more”. As Ofcom will be aware it can be difficult, if not impossible, to predict how long some incidents may last at the time they start or when we become aware of them. For the level of incidents Ofcom is talking about we would aim to resolve them within 12 hours, and therefore it is only on occasion that we would expect them to last long enough to fulfil Ofcom’s criteria from the outset.

45. There will be instances where we can predict that they won’t be resolved within 12 hours such as large scale cable faults or severe weather impacts, but for other incidents that aren’t resolved within 12 hours it is likely that it will only become apparent to us that this is going to be the case either after the 12 hours have expired, or close to that point, certainly beyond the 3 hour timeframe from the start of an incident that Ofcom requires. Therefore this criteria often can only be applied retrospectively, and Ofcom should make it clear in their guidance that they understand that CPs will report within 3 hours of the point they expect an incident to last more than 12 hours, rather than within 3 hours from the start of the incident. This guidance allows for a degree of subjectivity and judgment and Ofcom should show understanding of this when judging compliance against this criteria.

46. As outlined in paragraph 30 above, BT acknowledges that cyber-attacks fall within scope of section 105B where they have a significant impact on the operation of a public electronic communications network or service. However where there is no impact on the network they do not. For reasons previously explained Ofcom should remove the first of the suggested criteria relating to cyber-attacks, as any relevant incidents that should be reported to Ofcom will be captured through the other defined criteria.

47. As we have discussed previously with Ofcom (January 2016) the level of media coverage does not necessarily reflect the severity or impact of an incident. Section 105B of the Communications

Act 2003 specifically relates to incidents that significantly impact the network. It is entirely feasible that an incident that doesn't **significantly impact** the network could yet still lead to national mainstream media coverage, either through misunderstanding or misrepresentation of the facts, or due to other aspects of the incident. In these cases we do not believe that such incidents should be required to be formally reported as per Section 105B.

48. Nevertheless BT understands Ofcom's role as a public body and sympathises with their need to be fully informed in the case of media enquiries. Therefore since February 2016 where we have been aware of incidents that have attracted national mainstream media coverage that haven't already been reported to Ofcom we have endeavoured to do so and will continue to. However it is important to note that these reports will be reactive as we are unable to predict which incidents the media may choose to focus on.

49. Ofcom's definition of "national mainstream media coverage" could benefit from some clarification and direction given the increasingly disparate nature of the media. We presume that by 'national' Ofcom means UK wide and it would be helpful if Ofcom confirmed this. It would also be beneficial for Ofcom to define the term 'mainstream' and which media outlets, be they TV, radio, newspapers, online or other that they consider this encapsulates. These directions will help us direct our teams to build a process for monitoring and tracking media coverage.

50. Our press office already works quite closely with the press office at Ofcom. Given that we cannot predict which incidents Ofcom may receive press enquiries about we are always very happy to field questions from Ofcom's press office either through our press office or directly to the incident reporting teams as necessary.

Audit & Enforcement

51. In September 2016 the section 105C audit of EE examined a number of internal processes with relevance to security and resilience and its services. Ofcom had been considering EE's compliance with its security obligations under Section 105A of the Communications Act 2003. The audit was closed in December 2016. No follow-up investigation took place and no breach of General Condition 3 requirements was identified.

52. [✂]

53. So whilst BT understands the importance of Ofcom's audit powers in ensuring CPs abide by their obligations. It is important that Ofcom uses these powers appropriately. Such audits place a heavy burden on CPs in terms of time and cost, so where possible Ofcom should allow CPs the opportunity to satisfy any concerns Ofcom may have via alternative methods first. BT is concerned that Ofcom's suggestion that it may consider exercising its audit powers more often than previously (paragraph 4.7 of the consultation document) will lead them skipping this vital step that could satisfy Ofcom's objectives much quicker with less costs to industry.

54. Secondly in order to achieve Ofcom's objective of ensuring CPs are compliant with Section 105A Ofcom must ensure that the auditors it uses are instructed to communicate clearly and co-operatively with CPs. The scope of the audit must be clearly defined and understood by all parties to ensure effectiveness, and CPs must have the ability to raise concerns about the audit during the process and the ability to respond to any concerns raised by the auditors. The process must be designed so that CPs take it as an opportunity to ensure their own processes are

sufficient, and to learn and improve where they are not. If CPs feel the audit process is seeking to find faults and facilitate punitive enforcement actions then CPs may naturally become less co-operative with the audit process but more importantly the learnings may not materialise, or may not be taken in the spirit that ensures they are applied.

55. Finally the cost of an audit is an incentive for CPs to ensure that their processes are satisfactory and do not cause Ofcom concerns. However Ofcom must be careful not to overuse their powers, if CPs feel that Ofcom systematically audit them regardless of their behaviour, then the incentive to ensure compliance is somewhat diminished as CPs expect to face an audit regardless of their actions.