KCOM's response to Ofcom's Review of Security Guidance

Introduction

KCOM Group PLC ('KCOM') welcomes the opportunity to respond to Ofcom's Review of Security Guidance (the 'Consultation').[1]

KCOM considers that it is important that the negative impact of service outages are kept to a minimum and that communications providers ('CPs') face appropriate incentives to ensure that the public networks and services they provide are subject to effective risk management as well as being designed and operated in a resilient manner.

The Consultation is important to KCOM as changes to the security requirements currently applying under sections 105A to D of the Communications Act 2003 (the '2014 Guidance')[2] will affect our business. This is because we are a supplier of both Public Electronic Communications Networks ('PECN') and Public Electronic Communications Services ('PECS') not only in the Hull and East Yorkshire ('HEY') area but more widely across the UK. Specifically:

- In the HEY area we use our network to provide both wholesale and retail communications services to both residential and business consumers. These include fixed line communications services which we deliver using our current generation network and our next generation fibre network; and

- In the rest of the UK we to provide our consumer and SME customers directly using BT inputs; and to our wholesale customers using BT inputs.

Summary

- KCOM agrees that this is an appropriate for Ofcom to review its 2014 Guidance. Not only have both technology and operational practices evolved since Ofcom's current guidance was produced, there have been developments in terms of the cyber risk that warrant security considerations. In addition to these changes, Ofcom has also gained insight from the incident reports it has reviewed over the intervening period that have been submitted by CPs.

- Given Ofcom is proposing drafting changes to the 2014 Guidance the Consultation and describes changes and additions that are proposed as opposed to publishing the draft guidance. KCOM's view is therefore that Ofcom should

[1] Ofcom (2017), *Review of Security Guidance, Consultation on updating Ofcom's guidance on security requirements in section 105A to D of the Communications Act 2003*. Consultation, 30 June 2017, available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0024/103596/consultation-review-security-guidelines.pdf

[2] Ofcom (2014), *Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003*, Guidance, 8 August 214, available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0021/51474/ofcom-guidance.pdf

consult on the new guidance before it seeks to finalise it as the precise wording is critical.

- While recognising the drivers for change to Ofcom's 2014 Guidance, KCOM agrees with the central positon detailed in the Consultation that that the main elements of Ofcom's 2014 Guidance remain relevant to industry stakeholders and should be maintained by Ofcom in its new guidance. We also agree with Ofcom, for the reasons given above, that the 2014 Guidance should be augmented by adding to specific areas to reflect the heightened level of risks around security, or otherwise adjust the emphasis.[3] In doing so, it is important that Ofcom recognises that the strategic emphasis being proposed by Ofcom in combination with the long term drivers of change (e.g. climate impacts) not only have the real potential to increase the cost of regulatory compliance but also require a co-ordinated cross-sector response.

- The Consultation is helpful in highlighting the areas where Ofcom considers taking steps to manage cyber security risks to be an essential part of a CP's compliance obligations. However, CP's are being directed to take account of advice / guidance being issued by a range of institutions. It is therefore important that this advice / guidance is drafted appropriately and recognises the application.

- The Consultation is also helpful in highlighting the need for suppliers to take appropriate steps to manage the risks from flooding and power failure. It is appropriate for Ofcom to explicitly recognise the costs associated with risk management of these long term drivers which will need to be recovered.

- Ofcom's Consultation recognises the role that outsourcing can play in the provision of infrastructure which is used to support their networks. One of the central tools used in such outsourcing arrangements is the Standard Interconnect Agreement (SIA) between third parties and BT. In our view, now us the right time for Ofcom to review the SIA.

- Both Ofcom and government are seeking to incentivise suppliers to transition from current generation access networks to 'full fibre' next generation access networks (FTTP). We would encourage Ofcom to take this opportunity to clarify its position on battery back-up where these FTTP networks are used to deliver Publically Available Telephone Services ('PATS') and so must ensure uninterrupted access to Emergency Organisations.

- We have provided a more detail response to the Consultation below. We hope that Ofcom finds our contribution helpful.

[3] [Confidential: While KCOM recognises the increased emphasis placed on security, particularly in the cyber space, it is critical that where a CP is asked to undertake activities that there is a clear legal basis for doing so. Situations that fail to meet that test place CPs with clear difficulties.]

KCOM's response on specific points raised in the Consultation

1. Security and availability (s105A)

Cyber security

1.1. Ofcom note in paragraph 2.9 of the Consultation that it proposes to update the 2014 Guidance to recognise the creation of National Cyber Security Centre (NCSC), and to set the expectation that CPs should be aware if, and where appropriate be following, NCSC's guidance on relevant issues. Furthermore, Ofcom is proposing to explain that when investigating and considering enforcement action, in addition to general considerations such as those in the ENISA Minimum Security Measures,[4] it will also to NCSC for guidance on any cyber-security measures CPs should be taking.

1.2. In taking the proposed approach, it is important for Ofcom to ensure that the relevant institutions that are issuing guidance fully understand the basis on which their guidance is being given and that Ofcom sets a clear expectation on the timing of implementation of the measures to which it gives general consideration (e.g. ENISA Minimum Security Measures), as well as more specific contained in the guidance (e.g. NCSC). There is therefore clearly a role for Ofcom to work closely with these bodies to this end.

1.3. Ofcom will also be aware of the importance of effective penetration and vulnerability testing in order to secure data, especially with the General Data Protection Regulation (GDPR) coming into effect in May 2018.

Risk management and governance

1.5 KCOM considers it appropriate for Ofcom to add further details on its expectations concerning the risk management and governance of security risks, which includes reference to the processes employed by a CP in relation to its decision making about the management of those risks, as well as the level of internal security capability to ensure that those people considering the risks are appropriately informed.

1.6 As Ofcom notes, there are both compliance and commercial imperatives that drive a CPs decision to obtain Cyber Essentials (CE) and Cyber Essentials Plus (CEP) certification. In our view it is likely to remain a proportionate tool for a CP such as ourselves in demonstrating the steps that have been taken in adopted the relevant cyber security hygiene factors likely to be necessary, if not sufficient, for compliance with s105A. Furthermore, while we concur that CPs should encourage

[4] ENISA (2014), *Technical Guideline on Security Measures: Technical guidance on the security measures in Article 13a*, Version 2.0, October 2014, European Union Agency for Network and Information Security, Available at: https://www.enisa.europa.eu/publications/technical-guideline-on-minimum-security-measures

their supply chain to adopt the standards it would be helpful for Ofcom to explain where it considers the compliance boundary to lie for the purpose of meeting the obligations of s105A if parts of the supply chain do not adopt the standards.

1.7 Importantly, to the extent that a range of standards / frameworks (e.g. cyber vulnerability testing) are needed to demonstrate the sufficiency of compliance it is important to recognise the costs of these activities and as such the importance of avoiding unnecessary duplicate activities.

Cyber Essential Plus

1.8 We agree that Cyber Essentials and Cyber Essentials Plus certification is likely to remain proportionate for us to maintain (commercially and from a regulatory perspective) and we need to demonstrate the steps that we have taken to ensure that we have adopted the relevant cyber security hygiene factors in the event of an investigation. We are also being encouraged to adopt this within our supply chain, given it is aimed at all organisations, where it is proportionate to adopt it.

Minimum security standard for interconnection – NICC ND1643

1.9 KCOM is working with the NICC as part of its review ND1643, which concerns the minimum security standards for interconnection[5] The NICC review has raised a number of issues that are being addressed by the Security Task Group.

1.10 As suggested by Ofcom the NICC is intending to publish a Security Best Practice Guide is being developed in support of the All IP work stream. Ofcom has indicated that it would use this document as a reference point when determining compliance with s105(3) of the Act.

1.11 It would be helpful if Ofcom confirms how it would treat and new version of the standard from a compliance perspective.

1.12 As with other third party guidance KCOM considers it important that this documentation is clear and can be effectively used for the purpose Ofcom intends.

Cyber vulnerability testing

1.13 KCOM recognises that vulnerability testing used for cyber security purposes, such as the framework used by the Bank of England, has certain particular benefits.

1.14 We consider it important that where additional frameworks are introduced and potentially form part of a regulatory compliance assessment that:

[5] http://www.niccstandards.org.uk/current-work/index.cfm

- Ofcom makes clear that the information gathered through penetration testing would be used by it in any enforcement action; and

- wherever possible penetration testing does not serve to duplicate measures that form part of other standards.

Maintaining network availability[6]

1.15 KCOM considers it appropriate for Ofcom to amend its 2014 Guidance to reflect "all the appropriate" steps it considers CPs needs to take to comply with s105A(4) of the Act. In particular:

Single point of failure

1.16 KCOM considers that Ofcom is correct to recognise that the reasonableness of the 'appropriate steps' that a CP is expected to take to avoid single points of failure within the meaning of s105A(4) is a function of the points in a network, which Ofcom recognising by way of example of relevant considerations, including:

- It is more likely to be disproportionate to deploy protection paths in the access network than in a CP's backhaul and core networks;

- the number of customers relying on the single point of failure; and

- other issues such as geographic and physical constraints.

Flood resilience

1.17 KCOM was one of the participating CPs that took part in the National Flood Resilience Review, which resulted in investment in various measures to better protect against the risk of flood.

1.18 As Ofcom notes, the changing risk profile associated with climate change may need longer strategic response than tactical or operational measures. It is important that Ofcom recognises the costs associated with mitigations of this sort.

Power resilience

1.19 KCOM considers it important that Ofcom highlight the importance of CPs appropriately managing the risks of power failure to network availability in its revised guidance.

[6] We note that Ofcom is in process of reviewing its General Conditions of Entitlement and we would encourage Ofcom to use this as an opportunity consider how to approach the use of battery back-up in ensuring the availability of call access where PECNs are providing access to Emergency Organisations using full fibre networks.

Outsourcing

1.20 Given the decisions that Ofcom has taken in relation to outsourcing arrangements and the extent that these arrangements are used in the industry that it is important for Ofcom to confirm the position detailed in the Consultation. In particular:

(i) The regulatory obligations applying under s105A(4) in and of themselves to the cannot themselves be outsourced.

(ii) In principle, supply chain outsourcing arrangements appropriately constructed and risk managed can legitimately be used by CPs to provide infrastructure for, and to design and operate, their networks and that these arrangements.

1.21 We would further note that the industry makes extensive use of BT SIA to supply call access to Emergency Organisations. We consider that it is time for the SIA to be reviewed.

2. Incident reporting – Guidance on s105B

Mobile reporting

2.1 We recognise the need for consistent reporting of notifiable incidents and that all incidents are reported where one or more of the qualitative criteria are being met.

2.2 We agree with Ofcom's proposed method of calculating affected users on mobile networks in order to obtain comparable metrics. In our view strikes the requisite balance between obtaining sufficiently accurate estimates while at the same time avoiding unnecessarily complex calculations. Similarly, given Ofcom's stated purpose is to ensure consistency in reporting in our view it is advisable to use a common definition on which all mobile CPs are required to report against. For this reason, it is sensible to use either Ofcom's standard basis for classifying geotypes (i.e. local classification), or government (i.e. the Official Statistic used by Defra in its Rural Urban Classification).

Cyber incident reporting

2.3 It is clearly important that CP's recognise that cyber security incidents are within the scope of the incident reporting regime applying under s105B of the Act and have a clear understanding of the relevant basis for reporting and the relevant thresholds (i.e. those that have a 'significant impact on the operation' of a network or service), which include both qualitative (form) and quantitative (duration; and scale of service outage) thresholds. As Ofcom notes, the former could entail cyber incidents that result in major breaches of data confidentiality or integrity.

2.4 KCOM agrees that it is sensible to add a qualitative criterion to the list of reportable incidents as described in paragraph 3.32 of the Consultation as this removes any doubt that relevant cyber security incidents must be reported to Ofcom. This serves to punctuate the fact that where this form of incident has a 'significant impact' on the operation of services Ofcom should be made aware.

2.5 However, as Ofcom note there is a degree of subjective judgement involved in assessing whether an incident should be reported under the qualitative cyber security criterion applies i.e. one that has a significant impact. For this reason, we do consider that further guidance from Ofcom is warranted.

2.6 We note the proposed changes to the current incident "categories", whereby Ofcom is proposing three categories: (i) urgent (major); (ii) others that should be reported within 72 hours of us becoming aware); and (iii) non-major incidents that are typically those meeting the lowest fixed numerical threshold (to be reported in batches i.e. those incidents which commenced in a given calendar month need to be reported before the second Monday of the following month). We also concur that batched reporting needs to be undertaken on a routine basis.

2.7 Furthermore, KCOM recognises the need for timely reporting of incidents, with certain 'urgent' incidents needing to be reported as quickly as possible. This includes, but is not limited to, cyber-attack incidents that meet any of the qualitative criteria, incidents affecting services to 10 million end users; incidents affecting services to 250k end users and expected to last 12 hours or more; incidents attracting national mainstream media coverage; and incidents affecting critical Government or Public Sector services.

Incident follow up

2.8 Ofcom's Consultation noted that the 2014 Guidance identifies an incident follow up process depicted in Figure 3 of that guidance and that includes elements that Ofcom considers went beyond the incident follow up process itself, and moved towards enforcement.

2.9 KCOM agrees with Ofcom and with its proposal to truncate the incident follow-up process such that it stops at the stage of post incident analysis

3. Audit and enforcement

3.1 Ofcom's Consultation notes that in relation to specific incidents it will often be more effective to work informally with stakeholders, given that the priority will *usually* be to learn from incidents and avoid repeats. For this reason, Ofcom is proposing to truncate the current follow up process at the point of post incident analysis.

3.2 If stakeholders are to engage effectively in the manner Ofcom envisages it is important that stakeholders have absolute clarity on the basis of their engagement. This allows stakeholders to work with Ofcom in an open and constructive way with Ofcom, to learn the lessons from incidents that have occurred and to avoid them being repeated in the future. The use of the qualifier 'usually' leaves the question open.

3.3 Ofcom is also proposing to potentially use its auditing powers (that the CP being audited would have to pay for) more frequently and these would be used to find evidence of the measures that we have taken to manage a particular risk, in order to inform an assessment of whether there is compliance with s105A.

3.4 KCOM is concerned about the increased frequency of the use of audits. The existing basis for triggering an audit appears appropriate and proportionate. There remains a clear threat that investigatory activity may follow where a CP fails to evidence its compliance with s105A and 105B. It is therefore not clear why Ofcom's previous stance is no longer the right one and so on what different basis Ofcom is proposing to increase the use of audits.