KCOM Group PLC

Updating Ofcom's Guidance on Network Security
Call for Inputs

21 February 2014

Introduction

KCOM agrees that it is the right time for Ofcom to start the process of reviewing the current guidance on network security. CPs have now had nearly 3 years' experience of applying the guidance to their businesses and as Ofcom has highlighted technology and operational practices have evolved over that time. This coupled with the increasing importance of broadband services and an increased focus on security issues means that a review is timely.

However, we would be reluctant to see wholesale changes made which are not designed to either update the guidance to reflect current best practice or to address deficiencies in the current guidance. Providers already face a considerable burden complying with a variety of standards and we would not want to see that burden unnecessarily increased. Linked to this any requirements which are placed on providers need to commensurate with risk, i.e. related to the criticality of the services in question and the scale of the services being provided.

We are concerned that more prescriptive regulation has the danger of resulting in compliance becoming something of a "tick-box" exercise rather than a way of embedding best practice in a business. We are keen to see any changes to the current guidance reflect best practice rather than simply adding another layer of complexity to existing requirements.

In this regard, we believe it would be helpful for Ofcom to consider sharing data about incidents reported and trends with regard to network security at both a UK and EU level where this information is not currently provided. This would help facilitate knowledge sharing both of risks and how best to respond to them.

Below we respond to the questions which Ofcom has posed in the Call for Inputs with both our general thoughts and concerns more specific to KCOM.

Question 1 – What are your views on emerging and potential future security and availability risks and whether they should be addressed in the revised guidance?

The Detica report published alongside the consultation identifies future vulnerabilities such as:

- increasingly ageing infrastructure used in the network, including components that are no longer supported;
- a lack of complete understanding of internal network interconnections and dependencies, making incidents more likely to occur and to have a larger impact when they do; and

- less resilient equipment as a result of vendors attempting to deliver core requirements at the lowest possible cost as CPs drive down their service provision costs.

We accept that these risks are valid and in many respects are unavoidable as networks develop over time and knowledge is lost through personnel changes. As competition intensifies there is also the potential for timely investment in new infrastructure to be hampered due to cost pressures. The cost of providing resilience and market pressure to innovate and develop new products in quicker leadtimes also have the potential to heighten the risk from these vulnerabilities.

However, we believe it would be difficult put in place any guidance which could effectively deal with the any vulnerabilities arising as a result of historic network development. Specifics of these vulnerabilities may be unknown and beyond CPs dealing with them within their current risk management procedures and in line with the current guidance we are unclear what further can be done.

Likewise we are unclear as to what further guidance could be included with regard to potential future network vulnerabilities. It may also be difficult to understand, assess and manage any threats being introduced by interconnecting partners, even where interconnecting partners are already compliant with best practice standards.

Question 2 – In relation to the obligations to manage general security risks, how should our guidance be revised to reflect issues such as ENISA's Guidelines on security controls, supply chain management, the use of 3rd party data centres and applicability to smaller CPs?

KCOM would be reluctant to see the introduction of any new standards which might result in more onerous requirements and duplication of effort. In this regard, we already have a number of security related workstreams focussed on a range of different standards which require resource commitment and can result in a fragmented approach and act to decrease the overall focus on security. In this regard we note that the current draft of the ENISA Guidelines suggest they could be used as a neutral mapping to different standards in use by the industry, allowing providers to continue to use existing international standards and avoid incurring unnecessary additional costs. As a first step we believe it would be useful for Ofcom to map the ENISA Guidelines to existing standards in order to understand whether they in fact introducing anything new.

More generally, and to some extent less of an issue for KCOM, there may be an issue for international providers in having a separate requirement to comply with the ENISA Guidelines which are not an international standard that the US and other major trading blocks in the world will adopt.

We also note our understanding that BIS are looking to unify security standards. We believe that this is key in terms of the way forward – having one standard to comply with would simplify matters considerably. We would like to see Ofcom support and align with this but are unclear how compliance with the ENISA Guidelines fits into this.

Taking the supply chain issue, we are unclear regarding the extent of any changes Ofcom is suggesting should be discussed before finalisation. We appreciate that arrangements such as the network management outsourcing agreement which we have entered into with BT is one situation where we would expect to engage with Ofcom prior to finalising an agreement. However, we would have thought that as long as we were compliant with the "agreed standards" then this should be sufficient to prove that we had taken appropriate measures to secure our network. This would also apply in respect of other changes to the equipment and services supply chain.

Question 3 – How best can risks to end users be considered by CPs and appropriate security information be made available?

We agree that the provision of appropriate security information to end users is something which is currently often missed. This is probably due to a combination of factors - lack of interest on the part of end users and no one single view of the overall protection which a business provides to customers. We would be happy to provide additional information to customers but within an agreed framework with defined categories of information to be provided to ensure comparable and relevant information is being provided and at an appropriate level of detail. We would be reluctant to share details of vulnerabilities or the fine details of particular incidents but if we are to improve security holistically then we need make customers aware of incidents in our network and where possible help our customers to improve their own security.

Question 4 – Should Ofcom consider additional guidance in relation to network availability and the provision of related consumer information?

We agree that it may be best to refrain from attempting to specify exactly what information is provided to customers about availability and in what form. Real time information is readily available for customers who wish to seek it and providers will adopt different ways of communicating that information depending on their customer base. We also agree that it would be difficult to publish genuinely comparable and fair availability information on the availability of CP's networks.

Ofcom suggests that it may be useful to reflect the associated security objectives and measures relevant to the protection of network availability in the ENISA Guidelines in any revised guidance. We would refer to our earlier comments regarding the ENISA Guidelines and specifically the need to avoid any duplication of requirements and to map the requirements to existing standards before deciding that anything further is needed.

Question 5 – Would it be useful to clarify our expectations around reporting in the case of wholesale and "over the top" arrangements, and the need for CPs to maintain sufficient fault monitoring?

We believe it would be useful for Ofcom to clarify expectations around reporting in the case of wholesale and "over the top" arrangements and the need for CPs to maintain sufficient fault monitoring.

However, as Ofcom has identified, it is it is problematic for a network operator to apply incident reporting thresholds if the end users receive service via a downstream CP to which it provides network access on a wholesale basis. We are concerned about the practicality of a requirement to include end-users contracted with another CP who will report issues to the CP providing them with network access. In particular there will be complexities in assessing whether any of those end-users need to be included in any calculation of the impact of a specific incident, particularly one which is geographically limited in scale. Perhaps one way around this would be to require such customers to be included only where provision of wholesale services by a network operator has reached a defined threshold.

With regard to localised, often rural, outages which take a long time to be resolved, or persistently reoccur, we see no issue with Ofcom clarifying the need for CPs to maintain sufficient fault monitoring. However, we would be concerned if this were to introduce additional reporting requirements on CPs. In particular we note Ofcom's comments regarding outages which have not exceeded the quantitative thresholds but generate a level of complaints that are nonetheless "significant". We would be concerned if some further non-quantitative threshold were to be introduced for incidents of this type.

Question 6 – What are your views on the appropriate thresholds for reporting incidents affecting consumers of smaller CPs, mobile networks, data services and services suffering partial failures?

We agree that access to emergency services is a special case, and that the existing lower thresholds for reporting these outages should remain. We also agree that it would be timely to consider whether it remains appropriate to apply different thresholds for voice and "internet access" services. We also accept that the "internet access" description is probably too narrow to fully reflect the range of non-voice activities that consumers typically undertake and perhaps should be recast to more accurately describe the services being provided.

With regard to reporting thresholds based on absolute numbers of customers affected we are concerned that an alternative approach of setting some relative reporting thresholds would place an additional burden on small CPs where incidents currently fall below the reporting thresholds because of the total size of their customer base. We believe that the current thresholds are reasonable.

We are also unclear as to what additional guidance could be included to provide clarity on how to assess incidents resulting in degradation, rather than complete failure, of a network or service. We would like to understand better what "significant impact" Ofcom is referring to in these situations, particularly in the event that no consumers have experienced a complete loss of service. In our view these types of incidents are for individual providers to determine how to manage and communicate and should be adequately addressed through a company's risk management procedures without the need to report them formally.

Finally, Ofcom notes that it has not received any reports as a result of the application of the qualitative reporting criteria in the current guidance. Before determining whether there is a need to

give additional weight to these criteria or consider whether any additional ones should be included, Ofcom should at least establish that there has actually been failure to report using the existing criteria or customer impacting incidents have occurred which would warrant the introduction of new criteria. We would be concerned to see any changes made without evidence that they are needed.

Question 7 – What are your views on revising the current process for reporting significant incidents?

We have no particular issues with identifying a nominated contact point for reporting queries, nor with having a more tightly defined template for reporting. With regard to rejection of non-compliant reports, we would ask that Ofcom be very alive to the need to be flexible when a CP is endeavouring to report a major incident quickly. In these situations the priority for the CP will be ensuring that the issue is resolved as quickly as possible rather than ensuring strict adherence to a reporting template.

With regard to timescales for reporting we believe that it would be preferable for CPs to continue to be given flexibility in the reporting of the smallest incidents – either in batches or individually as they occur – rather than requiring that information be reported in batches. For major incidents, we agree that they should be reported as soon as possible and welcome Ofcom's recognition that a CP's focus will be on resolving the incident so that customers are no longer affected. In these circumstances we believe that the initial approach to reporting needs to encompass both formal reporting process but also provide flexibility to allow more informal notification of incidents and provision of updates such that Ofcom can be provided with the key relevant information quickly without essential resource being diverted from resolving the service issues.