

## Response of Vodafone Limited to Ofcom's consultation *"Updating Ofcom's guidance on network security"*

Question 1 .....	2
Question 2 .....	3
Question 3 .....	4
Question 4 .....	5
Question 5 .....	6
Question 6 .....	7
Question 7 .....	8

## **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?**

Vodafone considers that, while the traditional risks to both security and availability will continue to exist, it is likely that more intelligent/targeted attacks will become more commonplace. Changes in the way in which users communicate and share information, including, for example, an increasing emphasis on “cloud” services, support Ofcom’s recognition of a changing threat climate.

However, whilst Vodafone considers that the threat landscape is changing, it is neither necessary nor advisable for Ofcom to attempt to address each type of new risk in guidance, for two reasons:

- First, there is sufficient guidance on emerging risks already available through industry and government actors, such as the Cyber Security Information Sharing Partnership CESG, and the CERT community. An effort by Ofcom to provide separate guidance on threats would be an unnecessary duplication.
- Second, the rate of change is considerable, with new threats emerging rapidly and frequently. To remain accurate and relevant, Ofcom would need to update its guidance continuously, consuming Ofcom’s limited resource excessively.

Ofcom’s resource would be better deployed in providing guidance focussed on assisting operators in developing a toolset to aid in delivering compliance with the principles of the common regulatory framework, rather than on specific threats. By ensuring that operators maintain a suitable risk management framework, details of threats can be assessed and appropriate solutions determined, furthering Ofcom’s policy objective of building user trust in communications systems, without entailing Ofcom duplicating the outputs of other organisations, or expending resource unnecessarily.

**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?**

Generally speaking, it should be for each individual operator to ensure that its network and services are operated with an appropriate level of security, and that operators must have sufficient flexibility in the way they comply with regulatory requirements.

However, Vodafone welcomes the principle that Ofcom would reflect within its guidance those guidelines and standards developed by others, where Ofcom considers that they are valuable resources. This is clearly preferable over an investment by Ofcom in duplicating materials which already exist. In this way, Ofcom should be looking to promote adherence with existing standards, or promoting the development or expansion of existing standards.

In undertaking such an approach, it would be imperative for Ofcom to indicate how it considers that such guidelines and standards apply to the particular regulatory obligations at issue, and the extent to which meeting these guidelines and standards would evidence compliance with any given obligation.

Vodafone would also welcome clear and practical guidance from Ofcom on specific issues which Ofcom considers to be of concern, provided that this does not lead to expectations greater than those arising from the wording of the relevant legislation: any guidance issued by Ofcom must not have the effect of “gold plating” the various legislative requirements, and, to the greatest extent possible, operators must be granted the commercial freedom to implement measures to comply with regulatory obligations in the manner they see fit.

Such guidance would form an input to an operator’s overall risk management framework.

With regard to the proposal within paragraph 4.22 that an operator should consult Ofcom prior to commercial decisions regarding network procurement, Ofcom must develop clear principles delineating when such engagement is expected, with an established, published procedure setting out the risk assessment criteria which Ofcom would apply during such a process. Vodafone would be pleased to meet with Ofcom to discuss any proposals it might have in this regard.

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

Ofcom appears to be suggesting, in paragraph 4.40, that it should introduce a new obligation, requiring providers to make available information to customers around the measures taken to protect the security of networks and services. It is not immediately clear what, if any, evidence exists to substantiate a problem which necessitates regulatory intervention, nor, if there were indeed a problem, that the proposed solution is the proportionate means of dealing with it.

It is unlikely that most consumer customers will want technical details of how a particular network or service is secured, and that any proposal will require considerable thought and research as to how information might be made available in an understandable and meaningful manner, capable of being compared across operators, and across technologies. For example, to enable a customer to make a meaningful comparison between a fixed line broadband connection and a mobile broadband connection.

It must also be recognised that users may expose themselves to security risks which do not relate to the security of the underlying networks and services. For example, a user might install apps from an untrustworthy source, jail-break their device, fall foul of a phishing scam or otherwise be duped into disclosing personal details, or disable security in end-user equipment, such as running an open access point, or disabling a firewall to allow online interaction with a third party game.

It likely that the information which would be most helpful to the majority of customers would be some form of “assurance” rating, which can then be compared directly against the ratings held by others. Careful consideration would need to be given in terms of to how such ratings would be produced and the underlying evidence base assessed, without imposing a disproportionate obligation or cost on operators.

In any case, if, as Ofcom says, service security is a differentiating factor in consumer choice, the matter is a commercial one, and should be left to operators to address as they see fit. Vodafone has, for example, taken steps to enable customers — in particular, parents whose children may be far more technically knowledgeable than they are — to protect themselves online, by providing advice and guidance in Vodafone’s “Digital Parenting” magazine. See, for example, [Issue 1, at page 92](#). In addition, Vodafone offers a free app, Vodafone Guardian, to help parents manage their children’s smartphones.

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

As Ofcom notes, providing this information in a comparable and fair manner is likely to be difficult, although perhaps easier than with regard to network and service security; in particular, any proposed solution would need to take account of reliance on third party infrastructure, and network sharing agreements.

It might perhaps be helpful for Ofcom to promote a common approach by communications providers to provide some assurance of a high level of availability, such as certification against ISO 22301 (business continuity).

As is noted in the consultation document, it is entirely appropriate that due account is taken of services already provided by operators to enable customers and potential customers. Vodafone, for example, provides a publicly-available network status checker tool, showing the operating status of its network, along with planned and unplanned maintenance work, which is refreshed on a 30 minute basis:

Coverage checker

Network status

Type in your postcode or place name and we'll show you what's happening in your area.


SE1 9HA

Search

Unexpected issues

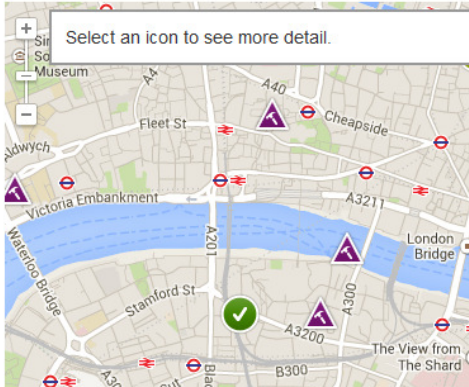
Planned maintenance

**See the work we've recently completed in this area:**



We've been doing some work on our network in this area to improve your 2G and 3G call and data coverage. Sorry if you noticed any disruption - we were working between 8am 24 Feb 2014 and 6pm 24 Feb 2014. ~

Select an icon to see more detail.



**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?**

Vodafone would welcome clarity from Ofcom as to expectations with regard to notifying Ofcom of security breaches. However, as above in response to question 2, Ofcom’s expectations must be grounded firmly in the statutory framework, and not amount to a “gold plating” of the law, which requires notification of a breach of security which has a significant impact on the operation of a public electronic communications or service (s105B(1)(a) and s105B(2)), or a reduction of availability of a public electronic communications network (s105B(1)(b)).

There is no legislative basis for the imposition of reporting obligations relating to a reduction in the availability of over the top communications services. As such, Ofcom would need to consider whether it was acting within the scope of its authority if it were to require network operators to notify of reductions in the availability of services such as BlackBerry’s email or instant messaging services, or Apple’s iMessage service.

If Ofcom were to desire reporting in respect of such services, Vodafone would expect Ofcom to place obligations on the relevant service providers (RIM and Apple respectively, in terms of those services mentioned above), not those operating the networks over which traffic pertaining to these services are conveyed.

With regard to reporting in a wholesale situation, Vodafone’s position is that the downstream provider should be reporting the incidents to Ofcom, as it will be best placed to assess the impact on the service it offers to its customers.

## 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?

### Thresholds for smaller CPs

Vodafone recognises the challenges inherent in both absolute and proportionate thresholds: absolute numbers means that few smaller CPs need to report incidents, whilst proportionate thresholds could overlook incidents where significant end-users are affected on large CPs' networks.

Since, for the purposes of larger CPs, the thresholds seem correct, Vodafone would suggest that a threshold-based approach is continued, but that Ofcom adopts a separate, lower, threshold for smaller CPs: such an approach should ensure that both small and large CPs report incidents of proportionate sizes, without excess reporting burden or under reporting.

### Mobile networks

Vodafone considers more than the thresholds in the guidance, when determining what to report. This includes the underlying impact on the customers, media interest and the like. Vodafone considers that the current regime works effectively, and would consider overly prescriptive guidelines to be detrimental. A more flexible approach, aimed at finding the right balance of reporting on a per-incident basis, would seem a more desirable outcome.

### Data services and M2M

Vodafone does not consider that a "one size fits all" to the reporting of incidents relating to data and machine-to-machine services would be sensible, given the wide variety of applications to which these services might be put. Inevitably, the criticality of some services will be greater than others, which has a considerable bearing on the proportionality of reporting obligations.

Ofcom would need to think carefully about what is appropriate, and Vodafone would suggest specific industry consultation and discussion prior to the drafting of any proposed guidance.

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

Vodafone supports Ofcom's position that, whilst it is important for reports to be filed expediently, reporting obligations should not divert focus from incident management and resolution. As such, any proposals to increase the complexity of breach reporting, or which have the effect of diverting focus, would be unnecessary and counter-productive. Whilst a more tightly-specified template may be appropriate, it is unlikely that this would be the case if the scope of information sought were to be expanded.

Similar, if Ofcom were to consider further an approach of rejecting reports, it would be incumbent on Ofcom only to reject reports where, in the circumstances of the particular incident, the omissions were so egregious that they caused actual harm. In particular, if a report were to contain the information which Ofcom required, albeit not in the preferred form, it would be disproportionate and unreasonable for Ofcom to reject the report.

If Ofcom is considering a change of template, it would be appropriate for Ofcom (a) to consult specifically on this, with reasoning as to why each change was required, to enable operators to comment on any operational impact, to ensure that it is fit for purpose, and (b) to operate a trial period, to test the new approach in an operational environment before committing to it.

Email remains a convenient way for submitting reports.