Updating Ofcom's Guidance on Network Security

EE's response to the call for inputs

28 February 2014

1. Introduction

EE welcomes the opportunity to comment on Ofcom's Call for Inputs. We recognise that the environment has changed since Ofcom first issued its Guidance in 2011 and so it is an appropriate time to conduct a review.

In summary:

- 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 the EE and its commercial partners.
- Network resilience reporting and information sharing already takes place through Government committees; therefore Ofcom should assume a supportive role in that process and not duplicate effort.
- As well as regulatory drivers for reporting incidents, there are commercial, corporate social responsibility and reputational drivers.
- Ofcom should adopt an outcomes-based approach where organisations must demonstrate that their security and resilience controls are fit for purpose.
- There is a lack of comparability of data provided by networks therefore Ofcom should refrain from making like for like comparisons.
- Ofcom must ensure that confidential and commercially/strategically 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 to Government.
- Ofcom must give consideration to that will ultimately bear the costs of introducing specific communications network security and reliability standards and the changes and upgrades to the equipment that is provided to industry.

2. Ofcom's overall approach and strategy

Ofcom's approach must take into consideration the highly complex nature of the mobile network and infrastructure. Mobile networks are far more complex in nature compared to fixed, where network configurations are virtually static connections which are changed generally only when a subscriber moves home and requires reprogramming at the exchange. Mobile networks, on the other

hand, are highly dynamic with the network configuration being re-arranged every time a subscriber moves into the coverage region of a different base station. Mobile networks must reconfigure themselves for users within small intervals of time (in the order of seconds) to provide roaming and imperceptible handoffs between cells, as a mobile moves around. Hence there is a huge difference between the nature of mobile infrastructure and everything needed to support it.

EE recognises Ofcom's duties in this area, as well as its desire for information in order to better understand how operators are managing and addressing the security and security and resilience vulnerabilities that currently exists, or could be anticipated in the telecoms network. However, MBG firmly believes that while Ofcom's perceives a benefit in its proposals, they will surely impose significant additional burdens on the mobile network operators, with no further benefit to industry or customers.

This is primarily because there are already existing public-private partnerships where information sharing exists between communications and other industries such as transportation. The forums include:

- CPNI (NSIE) where security incidents and vulnerabilities are discussed. The CPNI has already published papers on various subjects, including outsourcing and protecting data centres.
- EC-RRG forum which has the business continuity focus and includes emergency response management (the NEAT process).
- TISAC which discusses strategy.

3. Reporting Duty

CERT/ENISA already work on technical guidelines for minimum security measures and incident reporting. Issues relating to resilience are currently addressed by the ECRRG which was set up by the Cabinet Office and has fixed and mobile operators as members. As the information is highly sensitive, the individuals who are involved with this are all subject to Government security clearance. Ofcom must be sure that the information being requested does not overlap with information requested directly by Government.

4. Incident management

EE has its own internal processes and procedures which incorporate incident reporting. Each of the members has commercial and social responsibilities to their end users as well as commercial partners. These include:

- resolving Incidents within SLA defined quality levels;
- supporting the optimum availability of network and services;
- enabling the highest quality of service to customers;
- protecting revenue streams;
- providing information to support other processes within MBG; and
- providing data to enable process performance measurement (KPIs)

5. Treatment of Confidential information

Much of the information provided to Ofcom will be sensitive to individual companies. Therefore Ofcom would need to have the highest possible regard for protecting the legitimate sensitivity. This means that there should be protection against requests to release information using either the Freedom of Information Act or the Environmental Information Regulations.

6. Ofcom's questions

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?

It is evident that the more "traditional" risks posed to communications providers such as the dependency on a reliable electricity supply, infrastructure vulnerability to damage during severe weather events, and the impact of hardware failures, are as applicable today as ever. These are issues that have affected providers for as long as they have operated networks and services and every organisation will have gained experience in dealing these matters over many years.

The majority of fixed and mobile networks will have a Business Continuity Management team in place which may include Information Systems and Network Security teams within them (or independent of them) whose existence is to ensure that appropriate risk assessments take place and business

continues in the event of a major problem. As Ofcom states, we have to prepare for the possibility of more frequent and more severe extremes of weather in the UK, but there are also teams in place to anticipate a new generation threats. Mobile networks have thus already adopted a forward looking approach, but it is impossible to deal with the 'unknown unknowns' until they actually manifest themselves in some form.

Many of the risks highlighted by Detica in its report are already familiar to the mobile networks and have existed for as long as mobile networks have been around. As mobile networks evolve and infrastructure changes, they will continue to exist in different forms. No industry is completely risk-free and it is up to individual organisations to assess the risks in accordance with their own policies.

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?

In terms of incorporating any further controls within its guidance, or whether it makes reference to the ENISA Technical Guidelines, Ofcom should adopt a more outcomes-based approach towards compliance in this area. The mobile networks may choose to be more prescriptive in their own individual approaches, but the flexibility and choice remains for them to decide when considering compliance.

We recognise that Ofcom would like to make reference to a security standard governing the security and reliability of communications networks and services. However, as no such single standard exists that can be mapped directly to the network security requirements, rather than creating a separate dedicated standard, providers should be able to use existing standards such as ISO 27002, ISO 27011 and NICC ND1643. Many of the large providers can already demonstrate compliance with relevant aspects of the existing standard. We do not believe that it is necessary to create a new standard at this point in time, but if Ofcom (or BIS) is minded to take that approach it should involve the industry experts as early as possible in the process. This will ensure that all practical issues are addressed before it is too late to make changes. EE is very keen to engage with Ofcom and other mobile networks on version 2 of the ENISA guidelines.

Ofcom must give consideration to who will bear the costs of introducing specific communications network security and reliability standards and the changes and upgrades to the equipment that is provided to industry.

In order to ensure security is maintained across the supply chain and the costs are spread evenly, Ofcom would need to engage with all parties, not just the mobile networks. Existing contracts would need to be amended to reflect the requirements, should they come into force. EE does not believe that Ofcom should be involved in pre-approval of commercial or supply chain arrangements (whether material or not). We may choose to share important security information with Ofcom individually, if they have concerns. However, we should not be forced to seek approval.

EE welcomes Ofcom or Government engaging directly with third party owners and operators of third party data centres, with the objective of improving physical security. We also welcome Ofcom's recognition that approaches and their outcomes could have very different cost and proportionality implications for EE. Any obligations imposed in this area should be imposed directly on the data centre providers by Ofcom or the Government and not on providers who may not have the leverage to impose such requirements. Additionally, any changes in Ofcom's guidance will affect outsourcing arrangements which means that outsourcing partners would need to ensure that they comply with the updated guidance. The incremental costs of that will likely fall upon the communications providers. EE also believes it is right and fair to include smaller providers. In a networked ecosystem, the whole is as strong as its weakest link.

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

EE already takes security and availability very seriously. There are clear commercial drivers for this, but corporate responsibility and reputation management also play a large role. We do not believe that significant changes to EE's existing activity are necessary. End users can take comfort in the fact that EE works extremely closely with Government and are involved closely in national and international national standards setting groups such the ITU, 3GPP, NICC, etc. Information on security, if in the wrong hands, can create bigger risks for network operators which is why EE believes that it is not appropriate for security information to be made publically available.

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

Ofcom thinks that comparable data can be helpful to inform consumers and incentivise improvement (as is the case for fixed broadband speeds). Information can be divided into two categories:

- information about our approach to securing a given network or service; and
- Information about performance and quality of service.

Producing data for the sake of it is a burden on industry resources. It may also be difficult to produce information that is accurate and meaningful for the typical consumer. EE disagrees with Ofcom's proposal that publishing information on the availability of different providers' networks would be useful. Even if the published information may drive greater awareness among consumers of the importance of reliable networks, past experience teaches us that this sort of information is not used by customers because it means little to them and other features of an offering (price, services, handset and coverage) have a far higher priority when a customer is selecting a supplier. Oftel used to compile 'Comparative Performance Indicators' for the use of consumers but the initiative was abandoned, because it was so little used and the cost of preparation was not proportionate to the influence on the market. There have since been projects such as TopNet and Topcom which were also disbanded because of lack of consumer interest and comparability.

In respect of protecting network interconnections, EE welcomes proposal not to make major changes and that the existing approach remains the right one.

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?

Yes.

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

While EE acknowledges that there may be justification in having lower thresholds for 999/112 service, we do not agree that lower thresholds are required elsewhere. Any significant changes to the guidance are likely to have a significant commercial impact on EE, for example, an increase in staffing levels. We disagree with the proposal to use a network infrastructure based approach to setting mobile reporting thresholds, including an obligation to report by technology (e.g. 2G, 3G, 4G). However, there may be merit in reporting by

service, i.e. voice, data, etc. due to the growth in use, and importance of, mobile data services. With respect to outages affecting specific areas, we believe that consideration should be given to such reporting only where it is evidenced that significantly large areas experience service loss across multiple sites, i.e. causing significant disruption to a large communities or a large number of customers. This would need careful consideration in order to set the correct threshold and avoid placing an unnecessary reporting burden on operators.

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

EE agrees with Ofcom that major incidents should be reported as soon as possible. In these situations we also agree that it is important to receive information about the incident as quickly as reasonably possible, even though this is likely to have significant gaps. Also, a major incident for one organisation may not be defined as major for another organisation.

We urge Ofcom not to get bogged down in the administrative detail, such as an incorrectly completed template, but rather focus on the incident itself and resolution. We agree that small incidents can be submitted in regular batches and that major incidents should be reported as soon as possible.