Three
Star House
20 Grenfell Road
Maidenhead
SL6 1EH
United Kingdom

T +44(0)1628 765000
F +44(0)1628 765001
Three.co.uk

Three.co.uk

Ben Willis
Ofcom
Riverside House
2A Southwark Bridge Road
London
SE1 9HA

NON-CONFIDENTIAL

28 February 2014

Dear Ben

Hutchison 3G UK Limited (Three)'s response to Ofcom's Call for Inputs on Updating Guidance on Network Security.

Three is grateful for this opportunity to respond to Ofcom's Call for inputs on the update of its guidance on network security. Three's response will address some general points about Ofcom's overall approach and then answer each of the questions set out in the consultation document. Parts of Three's response have been drafted together with members of the Mobile Broadband Group (MBG).

General points and overall approach

Three welcomes the opportunity to comment and contribute to this discussion. We recognise that issues around network security have changed since Ofcom first issued its Guidance in 2011. However, we do not think circumstances have changed sufficiently to warrant or justify the introduction of further obligations on mobile network operators at the current time.

It is Three's view that Ofcom's approach must fully take into account the highly complex nature of the mobile network and infrastructure. Mobile networks are more complex than fixed networks in which configurations are mostly static connections changed relatively rarely, for example when a subscriber moves home which might and require reprogramming at the exchange.

By comparison mobile networks are highly dynamic. Three's network configuration is re-arranged every time a subscriber moves into a different coverage region. Mobile networks must therefore reconfigure themselves frequently and in a matter of seconds to provide roaming and seamless handoffs between cells. There are therefore real differences between mobile infrastructure and the technology needed to support it, and fixed infrastructure.

Three recognises that Ofcom have wide ranging statutory duties in relation to network security. We also recognise that Ofcom needs pertinent and comprehensive information to understand how operators are manage networks and address security and resilience issues, as well as future challenges facing the UK's telecoms infrastructure. However, Three is clear and understands that this view is shared across the industry, that, although Ofcom perceive benefit in their proposals, they impose significant and unnecessary additional burdens on operators, with no discernible benefit to industry or customers.

Three is confident of this view as the necessary public-private partnerships for necessary and appropriate information sharing already exist. These forums include:

- CPNI (NSIE) where security incidents and vulnerabilities are discussed.
- EC-RRG forum which has the business continuity focus and includes emergency response management (the NEAT process).
- TISAC which discusses strategy.

1. Ofcom's Reporting Duty

CERT/ENISA already have responsibilities in relation to technical guidelines for minimum security measures and incident reporting. Issues relating to resilience are addressed through the ECRRG which was set up by the Cabinet Office and has both fixed and mobile operators as members. As the information discussed by this group is highly sensitive, individuals who are involved are all subject to government security clearance. It follows therefore, that Ofcom must be certain that any information that they request does not overlap with information requested directly by government through either of these forums.

2. Incident management

As all operators do, Three has its own internal processes and procedures. These incorporate incident reporting. Three has commercial and social obligations to our end users as well as our 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).

3. Treatment of Confidential information

Three notes that under the proposals that 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 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.

In summary, three makes the following points in relation to Ofcom's proposals:

1. Three believes that the increased level of detail being sought by Ofcom in relation to information collection and incident reporting is disproportionate. We believe that the proposed measures will place additional and unnecessary burdens on Three and other operators.
2. Three notes that network resilience reporting and information sharing already takes place through government committees. It seems that Ofcom are seeking to duplicate this function which historically has worked well. Three believes instead that Ofcom should support the information sharing that already takes place and not unnecessarily duplicate this effort.
3. As well as regulatory drivers for reporting incidents, there are commercial, corporate social responsibility and reputational drivers.
4. Three believes that the most appropriate approach to the issue is for Ofcom to adopt an outcomes-based approach, under which operators would demonstrate that their security and resilience controls are fit for purpose.
5. Three questions the validity of Ofcom seeking to draw comparisons, as data holdings across operators are different and not of themselves comparable.
6. Lastly, 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.

Responses to specific questions

Q1 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 Three's view that the risks posed to communications providers around reliable electricity supply, infrastructure vulnerability to damage during severe weather events, and the impact of hardware failures, are as applicable today as they ever have been. These issues have always affected providers. Three, as every other operator, has gained valuable experience in dealing with these issues over many years.

Three like most operators has a business continuity management team in place which looks at information systems and network security teams whose purpose is to ensure that appropriate risk assessments take place and business continues in the event of major problems. We also recognise the possibility of more frequent and more severe extremes of weather in the UK, but believe we have the right teams in place to anticipate a new generation threat. However, we also recognise that 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.

Q2 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 an already complex compliance landscape with much duplicated content, we support the adoption of components of existing standards rather than the creation of new standards, where appropriate and justified.

However, 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 should remain for them to decide when considering compliance. Furthermore, any work in developing a new standard or approach, whether it is led by Ofcom or BIS, 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. Three would be happy to engage either individually or through the MBG with Ofcom on version 2 of the ENISA guidelines.

In order to ensure that security is maintained across the supply chain, 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. Three does not see value in Ofcom's involvement in the pre-approval of commercial or supply chain arrangements (whether material or not) although it may be appropriate for operators to raise issues individually with Ofcom. The MBG's members may choose to share important security information with Ofcom.

Three welcomes Ofcom and Government engaging directly with the owners and operators of third party data centres, with the objective of improving physical security. We welcome Ofcom's recognition that approaches and their outcomes could have very different cost and proportionality implications for operators.

It is right and fair to include smaller providers in a networked ecosystem.

Q3. How best can risks to end users be considered by CPs and appropriate security information be made available?

Three already takes security and availability very seriously. Three believes that it is in the interest of CPs and end users for network failures and security breaches to be mitigated. Experience has shown us that concerned end users will appreciate straightforward, jargon free advice delivered via a channel they engage with (not complicated statistics and comparisons).

Q4 Should Ofcom consider additional guidance in relation to network availability and the provision of related consumer information?

Ofcom think 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. Three does not see the merit in publishing information on the availability of different providers' networks. Experience teaches us that this sort of information is not used by customers because it means little to them. Other features of an offering (price, services, handset and coverage) are more important to consumers when making a purchasing decision. Three notes that Oftel used to compile 'comparative performance Indicators' for the use of consumers but the initiative was abandoned, as it was used so little.

In respect of protecting network interconnections, Three, welcomes proposals not to make major changes. The existing approach as set out in the 1022 statement remains the right one.

Q5. 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.

Q6. 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?

Three acknowledges that there may be justification in having lower thresholds for 999/112 services. We do not agree that lower thresholds are required elsewhere.

Any changes to the guidance are likely to have a significant commercial impact on operators (including increasing staffing levels). Three does not agree with the proposal to use a network infrastructure based approach to setting mobile reporting thresholds, nor do we support the introduction of a requirement to report mobile outages affecting a local area.

However, Three notes that as data services have increased markedly in importance, reporting of the most significant outages (in line with voice thresholds) should be introduced.

Q7 What are your views on revising the current process for reporting significant incidents?

Three agrees with Ofcom that major incidents should be reported as soon as possible, and within hours. 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. However, a major incident for one organisation may not be defined as major for another organisation.

We agree that small incidents can be submitted in regular batches and that major incidents should be reported as soon as possible, within hours.

Lastly, it is our view that Ofcom should consider redesigning the reporting template to include the use of predefined response fields. This will help to reduce the risk of misinterpretation or omissions in the data submitted.

We would of course be happy to discuss any of the matters raised further, if that would be of assistance.

Yours sincerely

pp C Raffinetti

Xavier Mooyaart
Head of Legal – Regulatory and Competition