Symantec Response to BIS Consultation on Proposed New Duties for Ofcom on Resilience Secondary Information

European citizens, industry and governments alike have become increasingly reliant and dependent on the Internet, mobile telephony and advanced communication infrastructures. The very foundations of Europe's modern society and economic stability are now built on communication infrastructures that span across national, European and international borders and the information that is shared, processed and stored within these networks. Given the way technology has become an integrated part of society the communications sector and the network and systems on which it operates has become a vital element of the UK's national infrastructure. Safeguarding these networks from possible attack or disruption has therefore become a crucial component of protecting the UK's critical infrastructure.

The requirement for Ofcom to conduct a full assessment and report on the UK communications infrastructure on a bi-annual basis in order to identify and mitigate issues of potential concern, as outlined in the Digital Britain report, was therefore welcomed. Symantec has also supported the steps being taken as part of the review of the European Telecommunications Framework Regulation to ensure the security, integrity and availability of network and services and protect the resilience and robustness of EU information and communications networks by taking a risk management based approach to security and having security polices in place.

The consultation documents recognition of the important role risk assessments can play in providing a means of identifying and addressing network resilience and security issues is also welcomed. Symantec see risk assessment as a proactive mechanism that can help organisations to effectively evaluate current threat and vulnerabilities and put in place appropriate counter measures. However, it is suggested that there is a need to ensure that any risk assessment requirement that may be introduced is sufficiently clear on the approach, criteria and measurements that would apply. Further clarification is therefore sought on issues such as the specific risk assessment approach and/or framework that may be applied and the criteria that may be used to determine whether the risk assessments undertaken are deemed sufficient and appropriate to ensure compliance with any requirement as introduced.

The following response aims to provide input to a discussion on how an effective risk management approach could be developed that is appropriate to electronic communication operators.

Do you agree that Ofcom should have the power to require that electronic communications operators report to Ofcom on risk assessments carried out?

A risk assessment is a proactive mechanism that can help organisations to effectively evaluate current vulnerabilities, identify upcoming threats and consider their level of risk, establish appropriate processes and procedures and define proper countermeasures. Conducting regular risk assessments is an important element of any organisations ability to identify, understand and appropriately address known, and unknown, risks they may be facing. Given the continually shifting and evolving online threat environment being faced by companies across all sectors having intelligence as to the risks and threats affecting key infrastructures in the UK is a key element to taking a proactive approach to protecting networks and systems. Only by understanding the latest threat or vulnerability can organisations prepare for risks and understand how to adjust defences accordingly to address the specific threat. Conducting a risk assessment can also help to raise the importance and visibility of security threats and issues to the executive and board level within companies.

However, further clarification is sought on the specific risk assessment approach or framework that operators may be required to follow to meet the requirement as outlined in the consultation document. For example a key issue not outlined in detail is the specific areas or aspects of an electronic communications provider's network, or operations, that will be expected to be the subject, or basis, upon which a risk assessment should be conducted to meet the Ofcom requirements. Furthermore whether a consistent single risk assessment framework will be developed upon which the risk assessment requirement will be based, and the possible timescales that may be involved in conducting the assessment and responding to possible security issues that may be identified and where action might need to be taken. The consultation document highlights the existence of the National Risk Assessment process and raises whether this could be used as a "starting point" or guide for the development of a risk assessment approach for communication operators. Symantec agree with the consultation paper that while the National Risk Assessment may provide a useful guide on the type of risks that Ofcom may be looking to identify and protect the communication infrastructure from, it was developed on the basis of the needs of government and therefore may not be fully appropriate. It is therefore suggested that further consultation could be conducted with industry, BIS and OFCOM to map the National Risk Assessment

already developed against the current threat environment facing the communications sector. This mapping exercise, or gap analysis, may help identify the key areas that any communication operators risk assessment could focus on. However, given the online threat environment continues to evolve and risks to the communications sector are increasing, it is important that any development of a National Risk Assessment process for the communication sector recognises that as risks facing communication operators evolve the risk assessment principles or processes introduced must also adapt to ensure all relevant risks are fully identified and assessed. It is also suggested that this consultation process should consider the risk assessment processes and practices that may already be being used by communication operators. This could provide an opportunity to highlight and build on examples of industry best practice, or existing self-regulatory approaches, that may already address Ofcom's possible requirements. However, any risk assessment requirement that is introduced should be technology neutral and only seek to outline the principles upon which a risk assessment should be carried out such as the criteria and assessment measurement that should be used.

Do you consider that Ofcom should have the additional power to require that further risk assessments be undertaken by relevant companies if those supplied are deemed insufficient. If so, how should this assessment process take place?

It is suggested that before being able to determine whether the risk assessment supplied by a company is insufficient, it would be necessary to first define what might be considered a "sufficient" risk assessment. Symantec believes that an effective risk assessment process should identify and evaluate possible vulnerabilities and threats to an organization operations and infrastructure and by doing so assist in defining appropriate and effective countermeasures that address these issues. While it is understood that each organisation involved in the UK communication infrastructure will have specific vulnerability profiles and may be exposed to different threats, a risk assessment approach could enable specific security plans to be developed that can address the unique level of risk being faced by that organisation. In addition an effective risk assessment should also identify and assess the interdependencies amongst different components, functions or systems within an organisations network and consider how a threat or risk to one element of a network could impact others. Given the interconnected nature of electronic communication network in the UK it is suggested that this is an important element that should be included in any risk assessment criteria developed for the electronic communication sector.

However, it is also highlighted that conducting a risk assessment is only one element of an overall risk management approach which is designed to assist organisations to take a holistic approach to understanding and addressing security risks on a continual basis. There are five essential steps involved in having an effective risk management process. These are:

1. developing an understanding and awareness of IT risks- by conducing a risk assessment
2. quantifying the impact on the business of these risks identified
3. designing solutions to mitigate threats
4. aligning IT and business processes to effectively implement solutions
5. monitoring, managing and continually assessing effectiveness of solutions put in place.

An effective, or sufficient risk management approach involves taking a pragmatic, holistic view of all the potential types of risk that exist. Once these risks are identified it is important to consider the possible impact that they represent. By doing so an organization is able to prioritize these risks according to the possible impact on their operations. Designing solutions that are appropriate to the risks identified is then possible. While it is recognized that the first step in this process is the focus of this consultation , it is suggested that the integrity, resilience and security of the communications infrastructure could be enhanced further by electronic communication operators being encouraged to take a full the risk management approach.

Regardless of whether a full risk management based approach is considered, Symantec believe it is important to ensure that risk assessments become a regular part of a company's activities. Given the constantly shifting threat environment it is important that risk assessment are conducted and audited regularly to identify and address new threats and risks facing networks and systems.

Should risk assessments be based on existing Government processes?

As highlighted in responding to question 1 the National Risk Assessment process developed for government could provide a useful starting point for discussing how an appropriate risk assessment framework and process could be developed. It is therefore suggested that these existing processes could form the basis for further investigation and discussion with the communication industry, and risk management experts, on how an appropriate risk assessment approach could be developed that may address Ofcom's requirements. Also it is suggested that communication operators may already conduct

risk assessments and have existing processes in place that may also be applicable and therefore should be considered and reviewed.

It is suggested that the approach and model used in PCI may possibly warrant consideration and discussion as it is understood that within the PCI model lower risk companies are able to conduct their own risk assessment and submit reports accordingly. These reports are then evaluated and if deemed insufficient the risk level of the company involved is evaluated and as a result they may then become measured according to the requirements for a higher risk company. For higher risk companies an objective third party assessment is required to ensure appropriate due diligence.

Symantec would welcome an opportunity to work with BIS and Ofcom to explore in more detail how a risk assessment framework and approach, appropriate for communication operators, might be developed on the basis not only of existing government processes but also current effective risk assessment practices being applied by businesses.

Do you agree there should be a duty on relevant companies to provide information to Ofcom on their emergency plans?

A modern approach to security and resilience of networks and systems must be a balance between protection from and preparedness for incidents. Having emergency plans in place therefore before any incident may occur is an essential element of resilience planning. For the communications sector in particular emergency planning is critical given the reliance on communication networks and the need to ensure emergency services, as well as citizens alike, to be able to communicate in the event of an incident.

Having a duty for companies to provide information to Ofcom regarding emergency plans could in fact act as an incentive to encourage companies involved in the interconnected communications infrastructure to ensure they take steps to prepare for emergency situations. Included in any requirement however should be a need to regularly test these plans and adapt them accordingly to ensure continued effectiveness and therefore preparedness for incidents. However, if such a requirement were to be introduced it would be important for Ofcom to assist companies by defining what would be considered an emergency situation to ensure the correct and appropriate plans are developed. For example a natural disaster, such as flooding could impact the communications sector, but also so could a directed cyber related incident. The incident seen in Estonia is an example of how a cyber based attack can have a “catastrophic” impact on a nation’s network and systems. However, the plans in place for dealing with a cyber attack and flood may be different and require different responses.

Also given the interconnected nature of the communications infrastructure in the UK it should be recognised that an emergency incident, such as those mentioned above, could not only have a significant impact on a communications operators but also impact and affect other providers of communication networks or systems. Therefore it is suggested that consideration also be given to the need to develop pre-arranged emergency procedures and plans not only between single operators and Ofcom but also between multiple operators in order to ensure critical communication services can be restored in an emergency situation both quickly and effectively.

Do you agree that there should be a duty on such companies to a) test emergency plans and b) participate in Government exercises as and when necessary to ensure overall resilience?

Symantec agree that having an emergency plan is vital and that providing information to Ofcom could assist in developing a collaborative approach where government and industry can work together when necessary to ensure critical communication services can be restored in an emergency situation. However, simply having a plan is not enough. It is important that companies regularly test plans to ensure they are effective against the threat environment. Following any test of emergency plans it is also important that lessons are learnt and that actions taken to mitigate risks or failures in plans that may have been identified. Therefore it is suggested that consideration be given to whether, following any participation in government exercises to test emergency plans, a follow up risk assessment may be needed to ensure all risks and threats identified in the emergency plan exercise, have been fully addressed.

Do you think that the proposals in this consultation document are in line with the expected outcome of the Framework Review?

The approach proposed in the consultation document is seen to be in line with the changes being introduced following the Telecommunications Regulatory Framework review. However the consultation document itself highlights areas where the Review may have taken a step further in introducing additional requirements to ensure the security, integrity and resilience of electronic communication networks. For example the requirement

for companies to have in place a security policy that is regularly audited and accessible to authorities. Symantec supports the moves taken in Brussels to introduce into the Telecoms Framework the importance of taking a risk assessment based approach to addressing security requirements of communication networks and the importance of security audits.

It is understood that the changes made in the Review have not as yet been finalized and therefore the introduction into UK law of the amendments may be seen as premature. However, this consultation is an opportunity for the UK to take a lead in highlighting the importance of protecting the resilience and robustness of communications networks by introducing the measures proposed by the EU that specifically address the security, integrity and availability of networks and services. Symantec would particularly encourage the introduction in any future UK legislation the requirement for communication providers to have in place security policies which are shared with regulators and regularly audited. In addition the requirement for communication operators to provide notification of a security breach that has impacted a network or services operations should also be introduced. This is seen as an important change to the European telecoms framework as it requires notification that a compromise in communication services has actually occurred rather than simply a predication or possibility that a risk may exist as outlined in the current telecoms regulatory framework. However, if the UK consider that this measure should also be introduced as part of this consultation process it is suggested that further consideration and discussion will be needed with industry on the possible need to develop guidelines on how operators are to determine when a security breach on a network has actually occurred and how significant a breach would have to be to trigger a notification requirement to Ofcom

Are there any other points you wish to make in relation to the issues covered in this consultation?

The consultation document highlights the intention to develop further policy work to consider the need for greater transparency related to outages and resilience incidents that may affect communications networks. Given the interconnected nature of communication networks and systems a key aspect of addressing the security requirements of critical national infrastructure, such as communications, is the sharing of information on incidents and the level of risks across shared networks and systems. Symantec would therefore be interested in participating and providing input into future policy work in this area to consider ways in which greater information sharing could assist in increasing the security, integrity and resilience of critical national infrastructures not only in the UK but across Europe.

October 2009

About Symantec

Symantec is a world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. Further information can be found at www.symantec.com.

For further information, please contact Susan Daley, Manager of Government Relations, Symantec, 62 Cornhill, London EC3V 3NH- tel. 07809 492 490 susan_daley@symnatec.com