



**Symantec Submission to EU Consultation on Critical Communication Infrastructure:
Availability and Robustness of Electronic Communications Infrastructures**

The pervasive nature of technology means that citizens, industry and governments are becoming increasingly reliant on the Internet, mobile telephony and advanced communication infrastructures (wireless, VoIP) to live, work and play. The very foundations of our modern society and economic stability are being built on electronic communication infrastructures that span across national, European and international borders and the data that is shared, processed and stored within these networks. Safeguarding electronic networks and systems from possible attack or disruption has become a crucial component of critical infrastructure protection. To do so however, requires a recognition that the concept of physical perimeter defence is of lesser value as critical infrastructure operations move away from closed, nationally protected computer networks to a more borderless, open, accessible, Internet-driven network environment. This shift in defence paradigm requires a change in the approach to critical infrastructure protection policy to ensure that issues that now impact and affect more than one nation are addressed effectively.

Symantec supports the consultative approach taken by the EU Commission on how best to protect the resilience and robustness of EU information and communications networks. Only by industry stakeholders and government working together can the security of the critical infrastructure within each Member States, across Europe and globally be protected. The opportunity to provide input to the study carried out by Alcatel-Lucent Bell Labs and partners is particularly welcomed. The report is an important document for mapping the current resilience and robustness of communication networks and considering possible actions needed to ensure the protection of these systems in the long term. The recommendations made in the report on how to enhance preparedness and the protection of increasingly interdependent networks are recognised as important for moving European discussion on critical infrastructure protection forward. However, to ensure all the issues regarding critical infrastructure protection are fully examined the following document outlines areas of the report's work and key recommendations that Symantec believe requires further consideration and discussion.

Guiding Principle and Methodology

We would like to highlight the fact that the report seems to be focused considerably on the traditional telecom and telephony network. As we described above we believe that internet technologies become more and more pervasive in our daily lives and that our critical infrastructure operators becomes more and more dependant upon them. The traditional telephony technology is also experiencing significant technological convergence into IP-based technologies. We therefore believe that it is important for the Commission to treat Internet and internet focused threats and vulnerabilities as a major area of research and further study in its policy development process.

Symantec believes the following strong assumption made by the report conditions the approach taken by the document; namely that threats are infinite and vulnerabilities are finite. As a result the report's main focus appears to be on vulnerabilities with the proposition that vulnerabilities can be identified and addressed through best practice. While it is recognized that the report does highlight that threats are also important, Symantec believes that this is a partial approach and, though it is true that threats are infinite, organisations and governments should, and must, prepare themselves to manage both threats as well as vulnerabilities.

Symantec believes that a modern approach to security must be balanced between protection and preparedness to Incidents. Even if vulnerabilities are finite, most of them are unknown or could be discovered at the same moment of a threat (zero days threats). Furthermore, countermeasures

are not infallible: for these reasons organizations must approach security as a pervasive process and must be prepared to promptly detect and manage security incidents.

Intelligence has a key role to play on this topic. Security needs to be proactive by seeking to understand what is the latest threat and vulnerability. In an environment of infinite threats and several zero day vulnerabilities it is critical to seek out the threat, be prepared for it and to adjust dynamically the defences that need to be flexible and intelligence lead.. The current paradigm is reactive based on responding to a known vulnerability for which often the threat is already out. The risk with the current situation is that often the response of most organizations is not fast enough to deal with the threat.

In the final report the methodology used to present the findings is based on a definition of a framework and a complete list of ingredients that make up a communication infrastructure. While this approach is not in question it is suggested, however, that processes, a fundamental component, is missing from the list used. Though processes are briefly covered under policies and human aspects, Symantec feels the report does not provide the correct emphasis on the importance of processes in critical infrastructure protection. It should be remembered that the leading security standard currently available, ISO27001 focuses on the role of processes only. If we consider a system as the sum of the infrastructures, processes and people it is clear that both vulnerabilities and threats can affect all three areas. Especially in the area of CIIP whereby there exist multiple levels of complexity, process is a critical component that can lead to successful defence or result in a security failure. In addition it is noted that the report does not highlight the importance of raising awareness, discussion and ultimately understanding amongst individuals working within critical infrastructures of the role of security processes and procedures to protect not only an organisations' operations but possibly a nations well being and ultimately a regions stability.

Report's Key Findings

Contained in the report are over one hundred findings. While the thoroughness, scope and depth of the work conducted by Alcatel-Lucent Bell Labs and partners is welcomed, there are some concerns over the usability of the final report. For example, the report has used two parameters to organise the key findings: maturity level and associated ingredients. However, it is suggested that this approach does not provide an organised or useful guideline to operators. Symantec believes that the only viable approach is provided by IT Risk Management.



Source: Symantec IT Risk Management Report: Volume 1 February 2007

IT Risk Management helps organisations to establish permanent processes to evaluate vulnerabilities, threats and to define proper countermeasures as outlined in the graphic below. . Every organization has a specific vulnerability profile (each infrastructure, organization and service is different) and is exposed to different threats. Risk Management is the only tool to define a specific Security Plan to effectively reduce the risks to levels that are acceptable by the organization. Also, IT Risk Management helps organisations to align IT to an overall business strategy and outlined in the illustration below.



Source: Symantec IT Risk Management Report: Volume 1 February 2007

The development of guidelines and best practices plays a key role also to raise awareness of new threats and vulnerabilities and to provide specific mitigation strategies to reduce risk. As outlined later in this paper, the inclusion of industry best practice in the report is welcomed. However, it is suggested that the seventy one best practice examples could be consolidated further to create a useful and accessible tool of guidance for critical infrastructure protection issues.

The following outlines Symantec's comments on the report's ten key recommendations.

1. Emergency Preparedness

Access to emergency services on an uninterrupted basis is vital not only in an emergency situations but on an ongoing basis. Given that current emergency services preparedness across Europe is believed to be largely informal, the report's recommendation to establish pre-arranged procedures and formal plans to restore availability and access to critical communication services quickly and effectively in the event of an incident is supported. However, it will be important that these plans are developed in partnership with industry partners that are increasingly in control of the systems and networks on which emergency service communications are based.

Symantec believes that in order to respond efficiently to an emergency, organisations should focus on the following:

- a. Risk Analysis: the organizations must be aware of the risks and their effect, following an all-hazard approach. Risk Assessments should be performed regularly, following a structured process.
- b. Impact Analysis: a fundamental building block of the Emergency Plan. It helps to identify and understand the interdependencies among all the different components, functions and processes of the organization and to determine which is the impact of an event that affects a single component to the Critical Services of the organisation.
- c. Constant Monitoring: organizations must establish proper processes to protectively monitor their critical networks in order to timely detect new threats. There are also external sources that could provide precious alerts (Rapid Alert Systems, Early Warning Services, Connection with National Centre for the Protection of the Critical Infrastructure, etc)
- d. Definition of an Emergency & Crisis Plan: the most critical part of an emergency plan is the coordination with external **interdependencies** (firefighters, police, external providers as power & water, civil protection, IT Outsourcers, other Telco Providers,

- Security Companies, etc.). The preparation of the plan must be done involving those parties. Periodical review of the plan should be performed with all parties involved.
- e. Simulations and tests: pilots learn how to manage emergencies through the continuous repetition of such emergencies. Organizations should follow the same approach. Periodical “war games” not only helps people of the organizations to be prepared to the emergency, but it provides also an assessment of the emergency procedures and their adequacy.

In addition it is suggested that consideration should also be given to developing procedures for responding to non-traditional attacks which may not lead to services being rendered inaccessible but where essential functions of emergency services that rely on technology are altered or manipulated remotely. Such a hypothetical scenario may be a critical emergency service online system or database being held to ransom by a Denial of Service (DoS) attack perpetrated using email. Increasingly systems being used to deliver essential emergency services have traditionally operated in a closed environment. However, the use of advanced technology by emergency services such as the police with networked mobile devices is resulting in a situation where governments are using the same technology, network and systems as the rest of society. For example medical services and hospitals are increasingly using email and Instant Messaging to communicate with and between hospitals regarding patient services. This means that services that are reliant on internet based systems and networks will be vulnerable to risks and threats that they have not had to respond to in the past. During July and December last year Symantec identified 46,929 DoS attacks against targets worldwide. In Europe the UK was the most targeted country for DoS attacks (49%) followed by Germany (11%) and France (8%). This data indicates that DoS attacks are a current threat to systems and networks across Europe and could have a direct impact on European critical systems and networks. A recent example of the power of a DoS attack was felt in early 2007 where an attempt was made to disrupt the Internet by launching DoS attacks on two of the Internet Domain Name System (DNS) servers. These servers provide the backbone of the Internet. If the attack had been successful the operations of the Internet and in turn all networked and internet dependent systems could have been significantly impacted.

Given the ever evolving threat environment and interconnected nature of the online community it is essential that Member States begin to understand how online systems are beginning to form the very foundations of modern life and therefore how emergency services may come under attack now and in the future from online threats. Fundamental steps should be taken to have in place procedures and processes to ensure critical systems are protected from possible attack. It is important however, that processes that are developed and implemented by emergency services are regularly reviewed and assessed to ensure ongoing effectiveness in light of changes in the online threat environment and the adoption of advanced modern technology by the emergency services.

2. Priority Communications on Public Networks

The ability of emergency services to communicate in the event of an incident is recognised as vital. The report’s recommendation for the development of propriety communication capability on future public networks for authorised callers is therefore supported. It is suggested that before any prioritisation can occur Member States should define critical services that will require access and agree a list of critical users. However, it can be argued that currently across Europe there is little understanding as to what defines a critical infrastructure even as demands for these infrastructures’ services increase. The current Commission proposal for Member States to define what constitute their national critical infrastructure in each key sector such as Finance, Power and Healthcare, is seen by Symantec as an essential first step towards building a secure response to an attack. Only by having this clearly defined can priorities for communications and actions in the event of an incident be determined and agreed.

Furthermore it is suggested that when critical users are defined and given priority communications in the event of an incident considered should be given to including IT system, software engineers and key employees involved in the provision and operation of communication technology networks and systems in any such list. These individuals will be vital to reestablish communication technology based systems in the event of an incident.

3. Formal Mutual Aid Agreements

European critical infrastructure is a patchwork of private and public operators, spanning across Member States. In order to effectively address the security challenges of Europe's critical infrastructure assets Symantec believes what is required is a co-operative approach among industry, government and law enforcement. Fostering co-operation and effective working relationships both within and between Member States is vital to ensure that all Member States have access to the expertise within the EU and that advice can be shared between those Member States that may be more advanced than others. Rather than the development of formal agreements which may be difficult to agree and formalise legally and may, in time, restrict the ability of industry and possibly governments to provide assistance as and when it is needed, Symantec believe a co-operative approach should not only be maintained but encouraged. This approach enables greater flexibility and scope to develop effective, responsive relationships that can meet the needs of Member States and provides support and assistance to key stakeholders as and when needed. This can be done through the creation of public-private partnerships, or widely accepted communication protocols or information exchange and preparedness/assistance schemes without necessarily taking the form of a formal legal agreement. Creating a trust environment and regularly testing the framework would be decisive factors in the success of this effort.

4. Critical Infrastructure Information Sharing

Symantec strongly believes that information sharing is a fundamental component of a modern ICT security strategy and a key component of protection in the current online threat environment. The threats we see today are dynamic, changing rapidly and therefore require unprecedented vigilance. The growth in new technical attacks grew in 2006 by 30% with threats and vulnerabilities from viruses, spam, phishing, identity theft and bot nets. Given this online threat environment it is important that those responsible for critical infrastructure protection have access to information on the emerging threat landscape. The latest Symantec Internet Security Threat report identified twelve zero day threats in the last six months of 2006. A zero-day vulnerability is a threat that may not have been known to vendors prior to exploitation, and the vendor had not released a patch at the time of the exploit activity. Zero-day vulnerabilities represent a serious threat in many cases because there is no patch available for them and because they will likely be able to evade detection. Given this shift in the online threat environment, having the right information at the right time could provide an effective means to guarantee a timely response to an attack on critical information and/or communication systems. Having real-time information collection, correlation, analysis and response capability can also identify abnormal or irregular behavior on networks that could be the indication of suspicious activity or even an attack to critical infrastructure systems.

It is important to highlight that information exchange is based on trust and for that trust to exist it is important that there is the appropriate framework involving people with the necessary seniority to take decisions. In addition information sharing needs to be done on a mutual basis and among all parties in order to foster that relationship of trust. It is of limited value to have an information exchange scheme whereby some partners come only to listen. This may require some cultural changes but is nevertheless necessary for the effective operation of such a scheme.

While Symantec agrees with the information sharing principles contained in Recommendation 4 we do however disagree on some of the indications. In particular Symantec believes that full mesh architecture will not help the organisations to benefit from information sharing. While it is true that a fully centralised architecture would create many obstacles, it can be suggested that the full mesh architecture supported in the recommendation would present more problems. For example, an evident obstacle is the number of connections among the different infrastructures. In a network of 150 operators there would be 22350 possible interactions (based on Metcalfe law). Another major issue is that every operator would have only a partial view of the online threat environment. Information sharing main purpose is to provide organisations and partners with a detailed map of the online environment that can then be used to take timely and effective decisions to react to, or where necessary counteract, possible attacks to systems and networks.

Given the important role of information sharing the report's recommendation of the establishment of formal means of sharing information between Member States and industry stakeholders is significant. However, while industry understands the importance of sharing information that could assist in protecting the critical infrastructure it must be remembered that companies operating under legal requirements and regulatory responsibilities may in fact be prevented from sharing information within Member States and cross borders. If formalised data sharing agreements are to be developed it will be vital that legal protections are put in place that ensure companies required to provide information are fully protected from legal prosecution and that any business sensitive information which are shared are protected.

An example of an effective information sharing system currently in place is the US IT- Information Sharing and Analysis Centre (ISAC) for which Symantec is a founding member. The IT-ISAC established a common standard for information sharing which provides systems and interfaces to allow information to be securely exchanged. This partnership ensures that organisations have a broader view of the online threat situation than any single organization and can provide early warning services to its partners.

The development of the proposed Critical Infrastructure Warning Information Network (CIWIN) would be a valuable tool to provide Member States with cross-border information on threats. However, Symantec believe this should not be limited to physical threats only but also cover the on-line environment.

To assist information sharing Symantec believe consideration should be given to the development of a common language for security incidents, response and escalation that can be used across sectors. This would enable Member States to act cohesively and ensure that sector threats which may impact a number of Member States can be dealt with efficiently. The ability of stakeholder to speak the same technical language in the event could help promote greater cooperation and also may assist in alleviating any challenges posed by the different technologies that the different providers may be using. In addition a common set of parameters for all Member States to follow for protecting interdependent systems in particular sectors could also provide essential assurance that efforts by one Member State to secure their own critical infrastructure assets are being met with equivalent efforts across national boundaries. Having common practices in place would enable response procedures to be developed, such as an escalation policy, where an incident is likely to require cross-border cooperation.

In support of this objective Symantec believe consideration should be given to the development of a common language for security incidents, response and escalation that can be used across sectors. This would enable Member States to act cohesively and ensure that sector threats which may impact a number of Member States can be dealt with efficiently. The ability of stakeholder to speak the same technical language in the event could help promote greater cooperation and also may assist in alleviating any challenges posed by the different technologies that the different providers may be using. In addition a common set of parameters for all Member States to follow for protecting interdependent systems in

5. Inter-Infrastructure Dependency

Given the cross border nature and interdependence of Member State critical infrastructure systems – from communications mechanisms linking Europe's citizens to water and power, to other Supervisory Control and Data Acquisition (SCADA) systems crossing Member States borders, Symantec believe the only means of securing Europe's critical infrastructure network is through a European-wide strategy. Such a strategy should involve all key stakeholders including government, law enforcement, relevant regulatory bodies and industry partners. Therefore the report's recommendation for increased engagement between Member States to identify, consider and conduct research into the extent of sector interdependencies is welcomed but should also ensure industry is involved in this research going forward.

Symantec believes that the identification of the interdependencies among the critical infrastructures is a fundamental component that presents some criticalities:

- a. Hidden or Indirect Interdependencies: not all dependencies are easy to identify. Organizations should focus not only on the important and evident dependencies, but also on those one that at a first glance are less critical
- b. Impact Analysis: the best approach to identify all inter-dependencies (both internal and external) is through an Impact Analysis. The analysis helps the organizations to link together all the different components and to understand how each one can affect the others, both directly and indirectly.

6. Supply Chain Integrity and Trusted Operations

The report highlights the security risks associated with the increased integration of online supply chains and the removal of established security perimeters leading to the need for increased end point security. While these are issues that are becoming increasingly relevant to critical infrastructure protection Symantec believe these issues can be, and will continue to be, managed effectively by implementing an information security policy that relies on a multi-layered defence against attacks.

In addition the report's suggestion that the development of innovative network operators and increase in the number of software providers, such as in the security environment, could lead to increased risks to the robustness of critical infrastructure is challenged by Symantec. Multiple providers in the market mean that specific attacks and threats can be identified and addressed by experts in those areas. Diversity in technology platforms is an important element of good security. Clearly no one company can react to all internet security issues that emerge and evolving. Therefore competition is necessary to ensure an innovative marketplace develops that reacts quickly and efficiently to new security threats. Having a mono-culture in information security could create a single point of failure, which can have a knock-out effect across the infrastructure.

The report's call for the development of innovative trust concepts that can provide assurances as to integrity of systems and the trustworthiness of networks will require further consideration and discussion to determine if such an ambitious proposal would be even possible. However, at present Symantec believes that trust in electronic services is best achieved through information assurance (IA). Good information assurance involves choosing the best practices for deploying people and using processes and technology appropriately according to the level of risk. Information assurance introduces processes and procedures for secure management of technology which is communicated to appropriate individuals with responsibility for the systems and networks. It must be remembered that technology alone cannot ensure online systems or critical infrastructure networks are secure. Raising awareness of online security issues and education are important elements of an effective information security strategy. Having IA policies in place also ensures that a system is not only secure and trustworthy when it is implemented but continues to be secure by being regularly reviewed and updated to cover the latest threats, tested to identify and address any weaknesses and enforced.

7. Unified European Voice in Standards

The concept behind the report's recommendation for Member States to co-ordinate efforts and present a common European stance when developing standards that can enhance network availability and robustness can be problematic and is very difficult to implement. There are currently multiple bodies producing different standards for particular sectors and industry's within each Member States, across the EU, and also internationally. Companies that are involved in critical infrastructure sectors, such telecommunications, financial services or energy, are required to adhere to multiple legislative, regulatory and standard requirements. Therefore it would not be possible for a common EU position to be developed on a standards issue which may need to be interpreted differently from one sector to another and where the standard may be appropriate to one Member States and not to another. In addition while the suggestion of developing an EU focus may create a more simple standards framework for companies to operate under, it is unlikely that European standards would remove the need for companies to conform to international standards; resulting in companies possibly having to face an increasingly complex and confusing standards framework. Moreover, security can be achieved in many different and sometime competing standards, methodologies and best practices. The establishment of a single standard does not guarantee better security and in fact is risking establishing vulnerabilities that

cut across infrastructures and products, thus creating a single point of failure, especially if the particular technology has “monoculture” characteristics.

8. Interoperability Testing

The development of a standardised network-to-network testing framework, that could ensure the reliability of new networks before joining existing networks, is a recommendation that requires further discussion and consideration. For example, it is questionable what impact the development of a test for new networks in the EU would have on critical infrastructure protection given that attacks do not emulate solely from EU networks; the interconnected nature and global reach of modern information communication networks means threat and vulnerabilities do not adhere to Member State or EU geographical boundaries. Interoperability testing makes good sense in any information technology environment when any new system is interconnected to another and should be part of the existing best practices. However in this case testing should not be limited only to interoperability but should also include vulnerability and security tests. The interconnection of any new system may introduce new threats and vulnerabilities to an existing one, some of which unknown. It is therefore essential element of good security that one tries to gain a good understanding of the additional risk to the infrastructure via such tests. Also, it would be vital that any criteria developed to test future network’s and used in the proposed “validation process” does not introduce technology mandates, particularly in the area of security, that could stifle European innovation and R&D. This may result in the EU’s ability to compete in the highly competitive global technology marketplace being restricted.

9. Vigorous Ownership of Partnering Health

With up to 90% of critical infrastructure assets in some countries privately owned and operated, addressing Europe’s security challenges requires a co-operative effort among industry, government and law enforcers. Symantec agrees with the report that building and maintaining the Public Private Partnership for critical infrastructure protection is vital. It is suggested that the establishment of a national Critical Infrastructure Protection authority (E.g. Centre for the Protection of National Infrastructure (CPNI) in UK) by each Member State could play an important role in fostering greater co-ordination and communication between key government and industry stakeholders in Member States on key critical infrastructure issues.

10. Discretionary European Expert Best Practices

The report’s emphasis on the value and importance of best industry led best practice to promote network reliability and security is supported by Symantec. There is clearly a role for industry and government to work together further to develop and promote existing best practice and, going forward, review and assess best practice as critical infrastructure requirements change and the defence paradigm continues to shift.

The development of a core set of voluntary best practice in the final report is welcomed. However, there is concern as to the usability of the seventy one examples currently outlined. While the document does categorise these best practice examples into specific areas (power, hardware, software, network, payload and policy) it is suggested that consideration be given to consolidating the examples to reduce the number from the current seventy one. By doing so it is suggested that the document’s best practice could become a more use and accessible tool for Member States to use when seeking expert advice and information on critical infrastructure protection issues.

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. Symantec appreciates this opportunity to submit comments on the Commission’s report. For further information, please contact Ilias Chantzios, Head of Government Relations EMEA, - tel. +32 (0)2 5311176 ilias_chantzios@symantec.com