BSA Comments on Improving Network and Information Security (NIS) in the EU

Introduction

BSA | The Software Alliance\(^1\) welcomes the opportunity to submit a response to the European Commission’s consultation on improving network and information security (NIS) in the EU. We fully support measures that will foster and promote a high level of cyber security not only in the EU but globally. Albeit BSA is not in a position to address some of the questions raised in the consultation, our comments highlight the factors and principles we believe are essential in developing a coherent and effective European Network and Information Security Strategy.

BSA member companies operate on the front lines of the digital economy – investing heavily in research and development (R&D) to provide software solutions and security tools to consumers, enterprises and public sector organisations of all sorts. We support initiatives that will bolster Europe’s cyber security capabilities by promoting market-driven technology innovation, agile and adaptive monitoring of cyber threats, and efficient coordination between public and private sectors.

Today, almost every aspect of the modern and connected world relies on the smooth functioning of information and communication technology. Citizens have come to rely and spend time on the Internet and use connected technology more than ever before\(^2\). The European Commission estimates that about 80 percent of young Europeans connect with each other and the world through online social networks and approximately USD $8 trillion changes hands globally each year in e-commerce\(^3\). Our essential critical infrastructure, such as the networks that manage energy, transport, finance and government systems, are interdependent, and are run by highly sophisticated and complex information technology systems. At the same time, these systems are faced with an unprecedented volume of sophisticated and complicated attacks.

Looking ahead, as consumers and governments increasingly take advantage of the economic and social benefits of cloud computing, users must be assured that industry providers

---

\(^1\) BSA | The Software Alliance (www.bsa.org) is the leading global advocate for the software industry. It is an association of more than 70 world-class companies that invest billions of dollars annually to create software solutions that spark the economy and improve modern life. Through international government relations, intellectual property enforcement and educational activities, BSA expands the horizons of the digital world and builds trust and confidence in the new technologies driving it forward. BSA’s members include: Adobe, Apple, Autodesk, AVEVA, AVG, Bentley Systems, CA Technologies, CNC/Mastercam, Intel, Intuit, McAfee, Microsoft, Minitab, Progress Software, PTC, Quest Software, Rosetta Stone, Siemens PLM, Sybase, Symantec, and The MathWorks.


\(^3\) European Commission Communication “Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre” (COM(2012) 140 final)
understand and properly manage the risks inherent to storing and running applications in virtualized environments, in contexts of high mobility, in the cloud. Likewise, cloud providers must be able to implement cutting-edge cyber security solutions without being required to use specific technologies.

Considered in total, improving cyber security is not just a question of improving trust and confidence in the various systems but is fundamental to the very basis of modern society.

**Scale of the Problem**

Information systems today must withstand a constant stream of increasingly sophisticated and malicious attacks. The perpetrators of these attacks range from well-financed organized crime syndicates to sophisticated hacker groups that launch attacks through millions of infected computers (“botnets”).

For instance, in July 2011, the US Pentagon, which houses one of the most protected and secure agencies in the world, acknowledged that it had suffered a major cyber-attack in which thousands of files were taken by foreign hackers. At the same time, many cyber security incidents and breaches are unintentional. For example, they can be committed by inadequately trained or insufficiently aware personnel. They can be caused by the use of inappropriate business processes, outdated security procedures, unsuited technologies, or even by otherwise adequate technologies being used improperly. Finally they can be, quite simply, the result of negligence.

- **Impact:** Cyber incidents and attacks have grown exponentially over the past few years. As the world becomes increasingly connected and reliant on computing and information technology, this trend will continue. The impact on the global economy is tremendous. A recently published cyber-crime report conducted by Symantec\(^4\) showed that more than 556 million users fall victim to cyber-crime per year, costing the global economy $338 billion a year. A further report by the National Cybersecurity Alliance and McAfee showed one out of five respondents indicated being a victim of crime over the Internet\(^5\).

- **Causes:** There is no single cause of security incidents; they vary from carelessness within an organisation (using infected USB sticks, opening unsolicited e-mails, failing to apply security patches, etc.) to massive, criminally motivated, cyber-attacks launched through botnets, or groups of malware-infected computers (also called “zombies”). The motivation behind these attacks is as far-ranging as the entities behind them. They can be driven by economic, political, ideological or purely disruptive (i.e., “hacktivist”) incentives. They often stem from well-funded and organized criminal syndicates that primarily steal valuable personal and financial information to resell on a thriving black market. In addition, security incidents also include industrial espionage (targeting companies’ intellectual property, R&D, business-sensitive information, etc.) and state-/government-sponsored espionage and sabotage. Highly motivated “hacktivist” communities (e.g., Anonymous) actively pursue their ideological goals through cyber-attacks.

---


\(^5\) [http://www.staysafeonline.org/stay-safe-online/resources](http://www.staysafeonline.org/stay-safe-online/resources)
Global nature of cyber security: Today’s global ICT networks connect everyone. Computing capabilities, telecommunications and the Internet now transcend borders, negating frontiers, reducing distance, and creating a global information society. The anonymity, global nature, ubiquity, device and system neutrality, interconnectedness and interoperability of the Internet present an ideal opportunity for criminals. Attacks can be launched from or into one or more countries using computers from around the world. The borderless nature of the Internet enables malicious individuals and groups to exploit loopholes of jurisdiction, making investigation and law enforcement difficult. Perpetrators can act from any location in the world and mask their identity, making jurisdictional borders as effective and relevant obstacles to law enforcement as they are irrelevant to cybercriminals.

How to Address it
Protecting cyberspace is a shared responsibility. No single entity or group of stakeholders can address the problem alone – and no individual or group is without responsibility for playing a part in cyber security. The technology industry, consumers, businesses and governments all must take steps to secure their own systems and to collaborate with one another to define and implement comprehensive cyber-security policies and technologies. A holistic approach is needed that ties people, processes and technology into a coherent Framework. All must play together; technology is only as effective as the process within which people use it.

Sensible Data Protection Measures within European Data Protection Legislation:
ICT security companies that combat botnets and other serious online security threats such as socially engineered targeted attacks must be able to process certain data to perform their duties and ensure network and information security. In addition, security systems and technologies deployed by a wide range of entities – including banks, hospitals, retailers, e-commerce web sites and governments – all process certain data to prevent malicious attacks and information security breaches. It is therefore vital that Europe’s Data Privacy laws allow such processing and provide legal certainty to critical infrastructure operators and their security providers on their ability to lawfully protect these systems. Data breach notification requirements, which are being introduced into Europe’s privacy legislation should be developed in such a way as to help organisations prevent and respond to security incidents while avoiding costly and burdensome rules that would not provide any real protection to consumers.

Improving Resilience and Response Capabilities: No system is 100 percent secure, and no technology or tool is without risk. Wherever there are commercial or destructive incentives, criminal elements will seek to find and exploit the vulnerabilities. Therefore an important element of effective security response is the ability to deal with incidents when they occur. This includes improving the resilience, preparedness and response capabilities through increased cooperation of European and other national Computer Emergency Readiness Teams (CERTs), Computer Security Incident Response Teams (CSIRT) and public-private partnerships. Furthermore, cyber exercises should be conducted nationally – as well as on European and international levels – on a regular basis.

---

6 Article 31 and 32 of the Draft European Data Protection Regulation.
basis involving both government(s) and industry participants.

- **Information Sharing:** A framework is needed that promotes voluntary sharing of cyber threat information, including close-to-real-time data, among and between companies and government bodies mutually. In order to achieve this, the framework needs to promote and help develop industry and government best practices. It should address legal barriers that may deter companies from sharing information (i.e. other legal requirements such as overly burdensome privacy laws) and provide incentives to stimulate industry participation in a trusted information-sharing environment. Such incentives should include allowing for the protection of the shared data according to its sensitiveness, protect trade secrets and intellectual property and provide adequate liability safeguards (e.g. under privacy, product liability and competition rules among others) when actors are sharing information for cyber-security purposes.

- **Research and Development:** Technological innovation combined with adequately skilled people and rigorous business and security processes are the best tool against cyber threats. As attacks become increasingly sophisticated, the pressure increases to develop new and advanced ways of combating them. A policy framework with a robust R&D plan is essential. It should encourage cyber-security R&D through European and national public funding of basic and long-term research, innovation and go-to-market support, and it should create incentives for the private sector to invest into cyber-security R&D. Public funding should focus on long-term needs by concentrating on circumstances where new threats are emerging, and/or where the technological solutions required are not yet commercially available, thus creating a measurable security gap.

- **Good Law Enforcement Capabilities:** Fighting cyber-crime must be made a top priority by enabling efficient and effective law enforcement, including allocating adequate resources to enforce cyber-crime law. National law enforcement authorities should sufficiently resource, and train investigators, prosecutors and judges, providing them with adequate equipment, skills, bandwidth, powers and collaboration mechanisms to conduct investigations that are highly technical, often time-sensitive and generally cross-border. Cyber-crime rings often have global operations, and law enforcement action must also take place across borders. It is equally important that law enforcement agencies build networks of relationships with their counterparts in other countries and regions. We believe that the new EU Cybercrime Centre is an important step forward in creating a central hub for cooperation, information-sharing and pooling of resources.

- **Software Piracy:** A 2009 BSA report shows a strong correlation between software piracy and malware infections. Markets with high piracy rates have the highest percentage of malware and infected computers. Security threats such as viruses, worms, trojans, and spyware often are designed to exploit vulnerabilities in common software products, forcing software developers to constantly develop patches and other fixes to keep emerging malware at bay. Typically, those who use pirated, unlicensed software (which often comes with malware embedded in it already from the start) are unable to access or download essential patches and critical updates that ensure their systems

---

remain as secure as possible. As a result, they are significantly more exposed to attacks and have much higher chances of being effectively hit. Furthermore, many peer-to-peer networks or websites that provide illegal software are also often hubs for malicious code that undermine IT security. Pirated software not only puts the user’s computer and data at risk, but the user’s computer can be used to launch large-scale attacks on other systems.

- **General Awareness Raising:** The Framework should promote good “cyber hygiene” through education and awareness-raising programmes. In particular home users, minors and small businesses, as well as the employees of any organisations, need to be made aware of the risks in cyberspace and encouraged to practice safe and ethical computing. This includes education about the dangers of pirated software use, risky online behaviours, sensible basic protection measures and actions. The framework should encourage Member States to fully use already existing industry resources for such efforts, as indeed industry – and the IT industry in particular – has developed a great deal of educational cyber-security materials, has marketing expertise and has established channels to communicate with the public.

- **Avoid Technology Mandates:** Security threats evolve extremely rapidly, therefore companies must be allowed to respond equally rapidly in creating and deploying new security measures. This level of speed and effectiveness would be compromised if the use of specific security technologies were to be mandated. Organizations must be able to deploy appropriate and cutting-edge security measures and technologies to effectively protect themselves against the actual risk(s) they are exposed to in the specific context of their own activities, which are different for every single organisation. Fostering a sound risk-management framework would thus be far more effective than technology-specific mandates. Organizations should be encouraged to assess their risk(s) and adopt security measures (people, process and technology) that are reasonable and appropriate to protect their systems. Doing otherwise and mandating specific technologies would both designate a single technology that cyber criminals must break or circumvent (a single point of failure) and at the same time give compliant organisations a false sense of security – whether the mandated technology is adequate to address the threats facing them or not. Furthermore, the Framework should avoid establishing preferences for any one business model or technology over another by enacting liability provisions for propriety technology. This would distort the playing field by creating incentives to forgo intellectual property rights and discourage the creation of proprietary software.

- **Risk-based Approach to Cyber Threats:** Consumers, businesses and government agencies seek to protect a wide spectrum of targets against a wide variety of cyber threats. A fundamental principle of effective security protection is that not all targets require the same level of protection, and not all threats present the same risk. Cyber-security policy should therefore enable consumers, businesses and government agencies to implement the security measures that are most appropriate to mitigating the specific risk they face.
➢ **Global Approach:** Cyber-security policy must recognize the borderless nature of the Internet, the global economy and cyber threats. As a result, a European strategy should promote government cooperation and ensure that national cyber-security policy frameworks integrate with global approaches and practices. Europe should continue to lead and encourage the adoption of the Council of Europe Convention on Cybercrime, which is an important step toward harmonizing national laws, improving investigative techniques and increasing cooperation among national law enforcement authorities. There are also examples of international initiatives such as DigitalPhishnet (information sharing on phishing) or the London Initiative on Spam that can serve as good models for future industry and government collaboration.

➢ **International Standards:** A policy framework should preserve the contribution of industry-led, internationally accepted standards to global cyber security. These standards not only underpin the global IT ecosystem, but they greatly contribute to cyber security by spurring the development and use of innovative and secure technologies. Mandating country-specific cyber-security standards, in particular standards developed by government agencies, may cut off a country's access to the most innovative, cost-effective and valuable security technologies offered on the global marketplace. There is an equally critical need for internal market-driven security standards on technological infrastructures. For example, the European Cloud strategy\(^8\) identifies the cross-border/global nature of the cloud; however it places greater emphasis on European standards over International Standards. This will lead to fragmentation, and the erection of unnecessary barriers that would jeopardize the ability to secure the cloud.

➢ **Avoid Creating Negative Incentives:** No other product in the world is attacked with the same sophistication and regularity as software. Yet at the same time, vendors have very limited control over how their software solutions are deployed, used and maintained or over the environment in which they operate. Even the most robust and secure information systems are only as secure as their use is proper. Therefore developing additional and disproportionate liability\(^9\), or imposing arbitrary minimum standards for software, would not only create legal uncertainty, but would also discourage investment into the further development of software, and would ultimately fail to address the reality of the cyber security challenge.

➢ **Notification Schemes:** Notification schemes, if properly implemented, can serve as an important instrument to enhance network and online security. For a notification system to be effective across all sectors, however, it must be workable and it should not impose unmanageable burdens on national authorities or businesses. Such a scheme should have the following characteristics:

  o **Harm-based approach:** On an average day, network and information systems must fend off thousands of attacks. Not all security incidents are the same or of the same severity. The seriousness of an incident should determine the need for

---

\(^8\) EC Communication (COM(2012) 529 /2) “Unleashing the Potential of Cloud Computing in Europe”

\(^9\) For example the current version of the Directive on Attacks Against Information Systems, which is still to be adopted by the European Council and Parliament, contains Recital 12b calls for Member States to “provide for relevant measures incurring liabilities in the context of their national law in cases where a legal person has clearly not provided an appropriate level of protection against cyber attacks.”
and level of response. In order to prevent “notification fatigue” for both recipients and the responsible administrative body, security incidents should be categorized according to specific harm or risk levels, and the notification requirement should be geared accordingly. Furthermore a harm-based notification principle can also create an incentive for businesses to implement stronger security measures.

- **Harmonisation:** In recent years, a number of Member States have adopted incident-reporting requirements either through voluntary or mandatory schemes. A harmonized approach based on common principles is needed as many cybersecurity incidents have cross-border effects and many service providers operate in numerous European markets.

- **Consistency:** A consistent approach and understanding of security breach is also needed within European legislation. Specifically, a security breach notification requirement was introduced in the 2009 adopted Telecoms Package (Art.13a of the Framework Directive and Art. 4 of the ePrivacy Directive), and similar provisions have been included in the Draft Data Protection Regulation (Art.30/31 and 32) and the Draft Regulation on Electronic Trust Services (Art. 15). It is important to apply a common set of standards in order to avoid different and competing reporting obligations.\footnote{See ENISA 2012 Report “Cyber Incident Reporting in the EU” (http://www.enisa.europa.eu/activities/Resilience-and-CTIP/Incidents-reporting/cyber-incident-reporting-in-the-eu)}

---

**For further information please contact:**

Thomas Boué  
Government Relations Director, EMEA  
at thomasb@bsa.org