CYBER SECURITY
INDUSTRY ALLIANCE

Response to European Commission Call For Input on the Forthcoming Review of the EU Regulatory Framework for Electronic Communications and Services

Addressing electronic data security policy options

January 31, 2006

CONTENTS

PAGE

1. INTRODUCTION

1.1 The Cyber Security Industry Alliance (*CSIA*) welcomes this opportunity to submit comments on the forthcoming review of the EU Regulatory Framework for Electronic Communications and Services. CSIA has placed particular emphasis in its submission on the security aspects of the Framework, and in particular the Directive on Privacy and Electronic Communications (2002/58/EC) (*Privacy Directive*).

1.2 A growing number of cyber-security threats have emerged in the years since the Privacy Directive was adopted. These threats have arisen from the growing sophistication of attacks on computer databases, servers, and telecommunications systems; the proliferation of new wireless technologies; the growing use of biometrics; and the convergence of communications networks, content, and electronic devices. Indeed, experts no longer track the gross volume of cyber security incidents because they literally occur on a non-stop basis. Databases at many European companies, linked by the Internet have incurred breaches by internal and external sources.

1.3 In 2005, the United Kingdom's Hi-Tech Crime Unit released a survey that found that more than 80 percent of 200 of the UK's largest businesses had been the victim of unauthorised access to their data networks. Many noted the sabotage of their data networks by company insiders as a key concern. Related issues of growing concern in the EU include identity theft and phishing. During 2005, Belgium suffered its first large-scale phishing attack, targeted at credit cardholders. Twenty-four European banks reported phishing attacks during the autumn of 2005 alone.

1.4 The EU Regulatory Framework should be reviewed in light of these developments and experience, so as to be able to protect users and ensure their trust in the systems.

1.5 CSIA would also like to underline the importance of considering this review in the broader political context, including the European Commission's *i2010: European Information Society 2010* initiative, the priorities of the Austrian and Finnish Presidencies in the area of information technology, and the recently agreed Data Retention Directive.

1.6 The European Commission's i2010 initiative has as its objective to foster growth and jobs in the information society and media industries. It is a comprehensive strategy for modernising EU policies to encourage the development of the digital economy by the year 2010. A recent survey of some 75 European business leaders and policy makers conducted by ENISA[1] shows that 90% of those polled believe that technology convergence and the move to an IP backbone will make Internet users less secure. Participants identified mobile security threats (38%), identity theft and phishing (21%), and denial of service attacks (12%) as the three biggest threats over the next five years. The right cyber security policies therefore have an essential role to play in achieving the goals of i2010.

[1] ENISA Quarterly, 10/2005 http://www.enisa.eu.int/doc/pdf/publications/enisa_quarterly_10_05.pdf

2. BACKGROUND ON CSIA

2.1 CSIA is an advocacy group dedicated to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education and awareness. Launched in February 2004, its members include the leading cyber security software, hardware, and service companies. The organization is led by CEOs from the world's top security providers, all international companies with a strong European presence. Its members include:

- Application Security, Inc.,
- Citadel Security Softwrae Inc.;
- Citrix Systems, Inc.;
- CA, International, Inc.;
- Entrust, Inc.;
- Internet Security Systems,
- iPass, Inc.;
- Juniper Networks, Inc.;
- McAfee, Inc.;
- PGP Corporation;
- Qualys, Inc.;
- RSA Security, Inc.;
- Secure Computing Corporation;
- Surety, Inc.;
- Symantec Corporation;
- Techguard Security, LLC;
- Visa International; and
- Vontu, Inc.

2.2 CSIA believes that a comprehensive approach to ensuring the security of information systems is fundamental to global protection and economic stability. CSIA’s goals include:

(a) Improving information security corporate governance.

(b) Establishing vulnerability disclosure guidelines.

(c) Reviewing cyber security best practices.

(d) Explore opportunities for cyber security R&D.

(e) Promoting existing international industry-led standards that protect electronic data from criminal activity and from unauthorized disclosures or uses.

(f) Enhancing international cooperation so that computer data has the equivalent level of protection is equivalently protected regardless of its jurisdiction or location.

(g) Reducing the risk of losses arising from data breaches.

(h) Promoting the resilience of critical Information Technology operations and systems.

2.3 CSIA believes these goals complement those set out by the European Commission in the i2010 initiative.

3. DIRECTIVE ON PRIVACY AND ELECTRONIC COMMUNICATIONS (2002/58/EC)

General Security Issues

3.1 CSIA supports the position of the Privacy Directive to set forth a technology-neutral standard for protecting the privacy of personal information used in electronic communications, and avoid specifying particular security technologies that might favor one mechanism or provider over any other. However, the Commission may wish to consider whether it would be useful to provide guidance, in the form of guidelines or best practice, of the types of measures that should be among those taken to provide sufficient security to meet the standards of the Directive. Such guidance could assist Member States and the private sector in taking practical measures to implement the Directive effectively.

3.2 Best practice could include encouraging the take-up and use of widely accepted international and European standards, without making specific requirements on the technical mandates.

3.3 An audit of existing security solutions might be a useful starting point for the consultation. Clearly, security solutions that reduce the risk of unauthorised access to computer databases and electronic communications are conceptual and not limited to particular technologies. While each one individually is useful when properly implemented and managed, one of the keys to reducing risk is to use multiple types of security solutions at the same time to provide a layered-defense. Given the current technology and threats, the major categories include:

(a) *Intrusion Detection*. Networks and servers hosting databases, like telecommunications providers, can use up-to-date firewalls, and intrusion detection and prevention software. Perimeter defenses such as firewalls have been recognized by industry as the absolute minimum cyber security protection and are seen as the starting point for a properly secured system. Installing intrusion detection technology on the database itself, as well as the network, provides an additional layer of protection.

(b) *Authentication and Access Controls*. Authentication is a process whereby a person or computer program proves their identity in order to access information. Proof of identity is generally given through at least one of three elements:

(i) Something the person knows, such as a password;

(ii) Something the user has, such as a smart card or electronic token; and

(iii) Something the user is, such as a biometric characteristic, like a fingerprint.

(c) Strong authentication requires at least two of these three elements. Once a user has been authenticated, access controls determine what privileges that user enjoys. Different levels of privileges, or users' rights, can be provided, and a given user may be granted some of these privileges, but not others.

(d) *Encryption*. Encryption technologies, properly implemented, can make it virtually impossible for unauthorized people to read data. Encryption obscures the data and requires a "key" to transform it back into a readable format. Encryption is another way to limit access to information to those people or departments that are authorised to have that access regardless of whether data is in transit, in use, or in storage. Databases with personal traffic data should be properly encrypted.

(e) *Monitoring*. Conducting regular penetration tests and audits of databases and routine management of all security controls are imperative. Knowing who accessed the information when, where and for what purpose is essential for demonstrating that an organization has taken appropriate steps to mitigate cyber threats. Monitoring and taking appropriate action where irregularities are detected are particularly important for knowing which data has been accessed and if and where the data has been transferred, for example to employee computers, mobile computing devices, or to external recipients.

IP Addresses and Personal Data

3.4 The classification of IP addresses under data protection legislatoin has received considerable attention at both the EU and national levels. The Article 29 Working Party and some national data protection authorities have suggested that IP addresses could constitute personal data. Such a conclusion could adversely affect the provision of security services and products. Security technologies often depend on IP addresses to prevent unauthorized access, denial of service attacks, malicious code distribution, spam, and to warn of impending attacks. By classifying IP addresses as personal data, legitimate security activities designed to protect such information under existing EU regulations will be extremely difficult. CSIA urges the Commission to provide clarity about the importance of IP addresses for network and information security.

Spyware

3.5 Spyware, or potentially unwanted technologies, is becoming more pervasive and complex. Spyware is often used to steal personal information. It does not spread in the same manner as a computer virus or worm. Instead, it infects a system by deceiving the user or exploiting software vulnerabilities. Many spyware programs trick the user, either by piggybacking on a piece of desirable software, or by deceiving the user into doing something that installs the software without him/her realizing. Permission to install such programs is often buried in overly complex “End User License Agreement”s (***EULA***s).

Removing spyware is often made difficult by hiding programs or making it impossible to uninstall such programs.

3.6 The current provisions of Directive 2002/58/EC do not appear to adequately address the issue of spyware or the means by which it is distributed. Rather than targeting technologies, CSIA recommends the Commission examine the issue of identity theft, which is often executed via spyware. The Commission should ensure there are adequate provisions in place for dealing with the online theft of personal information. The Commission should also provide protection legitimate anti-spyware firms from lawsuits. Those who propagate spyware or potentially unwanted technologies routinely sue security companies who remove – with consumers' consent – unwanted programs. A "safe harbor" provision would protect developers from such lawsuits provided anti-spyware firms apply a common methodology for classifying spyware and a dispute resolution process.

Breaches of Data Confidentiality

3.7 CSIA would like to suggest that consideration be given to the issue of breaches of confidential data, and what steps could be taken to deal with breaches. The Privacy Directive states expressly that there is a duty to prevent breaches and a duty to warn those whose information is at *risk* of being breached (Article 4(2)). However, the Directive does not define the term "breach" and only addresses the "risk" of a breach, rather than guidance about what to do in the event of an actual breach where data is compromised. It also does not provide guidance as to how to interpret the breadth of the disclosure requirement. In the absence of such a definition, different member states are likely to interpret the meaning of the word "breach" differently.

3.8 For example, is it a breach, requiring notification, when a hacker is able to enter an electronic system to add unauthorised information to that system, for example through spyware or an unauthorised cookie (for data-mining), but does not actually interfere with data relating to one individual's personal data? If such a case does constitute a breach, how broad must the notification be and to whom? To all users of the system? To only those persons whose data can be proven to have been disseminated without their authority?

3.9 There are risks in defining the term both too broadly and too narrowly. An overly broad definition for the term "breach," could, in light of the reality of daily assaults on electronic communications systems, cause an overload of reporting of routine and fundamentally unsuccessful computer intrusions to consumers and regulators alike. An overly narrow definition might not take account of the varied and complex types of breach that can occur.

3.10 The development of different standards by different data protection authorities within the EU in interpreting these issues could also create a substantial impediment to the free flow of information within the EU, and burden providers and data controllers.

3.11 In order to address these issues, the Commission may wish to consider launching a consultation with affected service providers, database controllers, computer security and information technology specialists and other interested parties in an effort to reach consensus on the critical issues of defining:

(a) What is a breach;

(b) When does the duty to inform come into place;

(c) Who must be informed of a breach; and

(d) What steps are considered sufficient to respond to a particular breach.

3.12 The Commission may wish to consider whether such a consultation should take into account the experiences of other jurisdictions beyond the borders of the European Union, which have been grappling with the complexities of the issue. In the United States, for example, there has been extensive legislative activity at both the federal and state level on this, with widely varying discussions and results. In the UK, the Information Commissioner recently had to consider this issue in connection with determining when sanctions are required following a breach.[2]

3.13 Reviewing this activity may be helpful in informing the Commission of relevant definitional alternatives and their potential consequences in light of actual recent experience.

3.14 CSIA believes there is also value in making information available to the public about security breaches that have taken place, the scope and frequency by sector, location, and technology for example. Surveys could be carried out by ENISA, in conjunction with the private sector.

4. AGREED DATA RETENTION DIRECTIVE

4.1 CSIA would like to take this opportunity to welcome the importance attached by the EU institutions to the issue of security, as demonstrated in the final text agreed by the European Parliament and Council of the European Union in December 2005 for a Data Retention Directive (Article 7).

5. BOOSTING SECURITY OF THE EUROPEAN INFORMATION SOCIETY THROUGH AWARENESS RAISING

5.1 Alongside this review of the Regulatory Framework, we think it is also useful to consider the issue of raising awareness of security. Whether shopping online, accessing personal records, contacting government agencies or browsing through e-libraries, ensuring data is securely stored and transmitted lies at the heart of any policy aimed at

[2] See e.g. "UK banks escape punishment over India data breach, Data protection watchdog investigation finds no evidence," January 13, 2006, at http://management.silicon.com/government/0,39024677,39155588,00.htm.

promoting the information society and building consumer confidence online. The issue of raising awareness of security, and educating users to use information communications technology responsibly must therefore be addressed. In this respect, work has been done through the Safer Internet Programme. More recently, the European Network and Information Security Agency (***ENISA***) held a workshop on good practice in awareness raising[3].

5.2 CSIA believes that the EU's success in promoting a secure European information society is likely to depend on its ability to achieve substantial success in raising awareness and educating users. There is a role for business and government to collaborate in this respect. Public/private partnership fora can help establish and monitor best-practice standards. Awareness raising tools include training in the workplace and via easy-to-use public access web sites where users can learn and also share experiences. The media can also be enlisted to publicize the importance of safe cyber practices.

5.3 Involving small and medium-sized enterprises (***SME***s) is seen as particularly crucial, as security awareness is often lower, resources are scarcer and smaller firms are likely to be among Europe's main job-creation engines. Given the diverse security cultures and standards across the EU's member states, creating common standards and best practices is vital in order to help spur economic growth and job creation. It may be appropriate to support further research and development on ways to lower the costs to SMEs of putting such measures into place, of seeking to understand what barriers exist today to the effective adoption of cyber security measures by SMEs, and of developing innovative techniques to facilitate strengthened security in this vital sector.

For further information, please contact

Paul Kurtz
Executive Director, CSIA
2020 North 14th Street
Suite 750
Arlington, VA 22201
USA
+1 (202) 204-0838
pkurtz@csialliance.org

Elizabeth Crossick
c/o Freshfields Bruckhaus Deringer
Place du Champ de Mars 5
1050 Brussels
Belgium
+32 2 504 72 45
elizabeth.crossick@freshfields.com

[3] http://www.enisa.eu.int/deliverables/index_en.htm