



Global Business Dialogue on Electronic Commerce

Cyber Security Recommendations

October 29, 2002

Leading Co-Chair (Asia/Oceania)

Dr. Hiroki Arakawa
Executive Vice President
NTT Data Corporation

Co-Chair (Americas)

Richard Brown
Chairman & CEO
EDS

Co-Chair (Europe/Africa)

Fernando Abril-Martorell
Chief Operating Officer
Telefónica

1. BACKGROUND

The issue of cyber security has been one of the central parts of the GBDe work program since its origin. Since that time an effort has been made to promote a harmonized policy infrastructure to enable a robust and globally integrated e-commerce system capable of responding to threats in a coordinated and timely manner. In 1999, the Authentication and Security Working Group made a recommendation which focused on developing key principles including "Protection" and "Promotion". This recommendation was followed and supported by the GBDe Cyber Security Recommendations of 2000 and 2001, which mentioned the interoperability issue of digital signature and certification authority.

In 2000, the GBDe continued to examine the broader issues associated with cyber security and the prevention of cyber crime.

The recommendations of 2001 addressed issues and messages to governments and industry, and a set of recommendations was developed urging greater coordination between the private and public sectors. These recommendations were based upon the understanding that the solution of cyber security issues requires strong cooperation between business and government. For this

reason, the GBDe sought to define the extension of the relationship between business and government in this area.

After making these recommendations, cyber security issues were faced with the following significant new trends.

1. September 11

Although the attack of September 11, 2001 was not cyber terrorism itself, it created national interest in security in all fields, including cyber security. Not only the protection of information systems from the threat of terrorism but also from national espionage has attracted world attention and, furthermore, surveillance for cyber crime and human rights issues, including data protection, have become relevant topics since September 11.

2. European Cyber Crime Convention

As the GBDe recommended at the 2000 Miami Annual Conference, an international legal framework to combat cyber crime is necessary and such a framework should focus on comprehensive international solutions which are carefully tailored and balanced, taking into account the expertise and adequate involvement

of industry. Each government has continued discussions on how to establish such framework domestically and internationally. In November 2001, the Council of Europe adopted the Convention on Cyber Crime⁵. In order to fight cyber crime, there is a need to clarify what constitutes an offence or a crime, especially when we speak about a global scenario where definitions of illegal activities pursued worldwide are needed. Governments should agree on the definitions of certain crimes committed in the Internet environment.

Although there is a global agreement to work against child pornography, there are other crimes like money laundering, fraud, denial of services, spread of viruses and other related activities that should be agreed upon and condemned as crimes. There is a need to agree on the definition of what are the major dangers to the Internet. The European Convention on Cyber Crime should be implemented in a manner that balances the need for effective law enforcement with privacy and other important considerations.

3. Increasing damage by viruses and cyber attacks

The more people use the Internet, the greater the chance for increased cyber attacks and viruses. In East Asia, for example, always-on access to the Internet by Digital Subscriber Line (DSL) has multiplied the number of computers and information systems damaged by viruses and cyber attacks because many computers and systems are not sufficiently protected to face being connected to the Internet 24 hours a day, seven days a week. A similar situation may also occur in other areas outside of Asia (e.g., Eastern Europe, Africa, and Latin America), where the use of the Internet by DSL is expected to grow in the coming years.

1. CULTURE OF SECURITY

With respect to the new trends in cyber security, governments and international organizations have made further efforts to promote cyber security policies. Governmental concern has focused on a number of issues including combating and preventing cyber crimes, protecting critical infrastructure against cyber attacks and improving the security of government information systems. These legal and legislative activities have come to be discussed globally and therefore, international harmonization is also being considered.

⁵ For more information visit:
<http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185>

In addition, many government initiatives for promoting Information and Communication Technology also mention cyber security as one of the top priority issues. For example, "e-Europe 2005" states that the private sector should develop good practices and standards and promote their consistent application in the context of "culture of security"⁶. The "e-Japan Priority Policy Program 2002" emphasizes "ensuring the security and reliability of the advanced information and telecommunications network" as one of priority policies, which recognizes the role of industry as important to some extent.

Government activities in cyber security have reached a new phase of development with the initiation of international business discussions to begin combating cross-border cyber crime. The private sector has also been involved in dialogues to investigate new methods and ideas in cyber security.

In addition, governments of the Organization for Economic Co-operation and Development (OECD) have drawn up new Guidelines for the Security of Information Systems and Networks. These guidelines are designed to develop a "culture of security" among government, business and users in an environment of worldwide expansion of communications network, increasing interconnectivity across national borders, converging technologies and ever more powerful personal computers.⁷ The G8 clearly supports and endorses promoting and implementing these new OECD Guidelines.

It is expected that the Internet will expand much more in all regions of the world with all kinds of users and that all generations will join the Information Society through the Internet. In such a situation, cyber security should be established as a significant part of information infrastructure worldwide. Cyber security should be implemented in a manner consistent with the values recognized by democratic societies, which include the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency. To realize cyber security, all stakeholders of the Internet (governments, industries, academics, and personal users) should be aware of the need for information security and what they can do to enhance it. They are responsible for the security of information

⁶ eEurope 2005: An information society for all, COM (2002) 263 final, 28 May 2002. Proposed actions of "3-1-3. A Secure Information Infrastructure"

⁷ <http://www.oecd.org/EN/document/0,,EN-document-13-nodirectorate-no-12-33186-13,00.html>

systems and networks, and, therefore, should be accountable in an appropriate manner depending on their individual roles. For example, governments should establish legal and regulatory frameworks for public security, and provide secured information infrastructure as public services. Industries should not only develop and invent more secure technology for information and communication, but also adopt a comprehensive approach to security management.

For these reasons, the GBDe respects and endorses the OECD guidelines which were finalized through a discussion that has included representatives of industries, consumers, and civil society. The guidelines should provide a new framework for governments, industries, and consumers worldwide to join and enjoy the benefits of the Internet and Information Society.

Under these circumstances, the GBDe supports and endorses a “culture of security” from the GBDe’s own perspective.

1. To propose a Framework for Cyber Security Discussions

There are many cyber security issues, and the greater the dialogue between government and industry to find solutions, the more often these issues arise. This year, the GBDe Cyber Security Working Group put cyber security issues into three categories depending on the respective roles of government and industry. The GBDe expects that the following structure will promote the discussion in other domestic and international fora, both for government and industries.

a. National Security

Combating cyber terrorism, protecting critical infrastructure against viruses and cyber attacks, national espionage, and related issues are a high priority for governments. Governments should take active initiatives on these matters taking into account the interests of industry. Industry should, in turn, cooperate with governments to find the best solution. The solution should not result in increased burden or the imposition of higher costs for business development.

b. Public Security

Cross border cooperation between law enforcement and international legal infrastructure for combating cyber crimes is crucial in making progress on this issue. Also for this kind of issue, governments should take initiative for settlement and industries should support government initiatives, which do not present an obstacle to business development.

c. Security for industries

There are many cyber security issues which companies should make efforts to resolve; for example, protecting information systems or enforcing security policy for security management among others. This kind of issue should be called “security for industries” and governments are expected to support such industrial activity and effective efforts.

2. GBDe Recommendations for Characteristic Features of Cyber Security

a. Global and International approach

Governmental approach in cyber security can be different in each country and region because of cultural and social diversity. By developing a common approach in global dialogues, such legal frameworks could be harmonized effectively in order to prevent cyber crimes, considering its cross-border nature. The GBDe expects each country to cooperate with each other through international dialogue, and an international approach should emerge from such efforts.

b. Business Approach

Industry could support such inter-governmental initiatives and, furthermore, industrial approaches are necessary and should be taken into account. The GBDe expects that government approach in cyber security should recognize the importance of industrial approach, which should be included as part of IT developing policies by government.

Through these discussions, the GBDe expects cyber security issues to be recognized as significant for IT development, and the relationship between government and industry to be clearer. The GBDe makes the following recommendations regarding “Culture of Security” as a part of the GBDe approach.

THREE ELEMENTS TO CONSIDER

1. Security & the Business Enterprise

Information Security is a crucial issue for business enterprises. Businesses need to protect information systems from external and internal attacks as key elements in their business operation; their activities are exposed to the risk of being damaged by possible attacks on critical social infrastructure, as the world becomes more and more dependent on broadband Internet access. These issues are important in terms of risk management, and directors and senior management need to be clearly informed about these issues.

Therefore, industry should encourage the creation of a "culture of security compliance" across all sectors. Most users are not aware of the extent of damage a single virus could cause both in economic terms and by harming infrastructure. Also, an employee acting without due diligence in his/her job could cause the same harm as if he/she had intentionally launched an attack against certain infrastructure. For these reasons, the GBDe recommends that industry develop online programmes with the task of educating users as well as workers on the importance of developing a Safe Network Environment. The more people that are educated on a culture of security compliance, identifying types of attacks or reporting illegal activities, the less the chances of their businesses being harmed by a cyber attack

2. Collaboration & Internet Protection

Business enterprises and governments are expected to collaborate both internationally and locally in order to protect the Internet from external attacks. Specific goals include the promotion of voluntary information sharing on cyber crimes and cyber attacks within industry, with the assistance of governments, and the close cooperation of industry with investigation authorities on various responses to cyber crimes.

At the same time, it is important to limit the burden on industry in cooperating with investigation authorities, as the GBDe stated in European Forum discussing the Convention of Cybercrime.

3. Poverty & Security

Attacks against information systems are one of the major obstacles hindering the development of electronic commerce and the Internet. These activities not only harm consumer confidence in the use of the networks as a new tool for business, but also impose an economic burden on the private sector and on the public bodies and consumers, which threatens to make information systems more costly and less affordable for users.

The issue of security is fundamental when seeking a good implementation of information society services in developing countries. Experience in developed countries has shown that consumers are reluctant to use electronic commerce if the network is not reliable enough to protect electronic transactions or the transfer of confidential information. Thus, a secured network is more reliable for users and consumers. Therefore, to achieve the rapid implementation and use of electronic commerce in developing

countries, it is necessary to take proper measures regarding the protection of personal data, secure electronic transactions and security of networks.

The GBDe recommends that developing countries and economies work towards the creation of regulatory measures that would ensure minimum standards of protection for confidential information, security of networks, and security of transactions.

2. RECOMMENDATIONS

1. Certification and security standard

In order to enhance the quality of information network security - standardization of response measures, risk assessment, and security management, enhanced by education and promotion - it is essential to focus on security measures themselves. Higher perception of information security by network providers, individual users or SMEs improves the quality of security throughout the network and makes it less susceptible to viruses and cyber attacks.

On the issue of standardization of security measures itself, the GBDe has recommended the promotion and required interoperability of digital signature and public key infrastructure, which are bases for global electronic commerce. There exist as many methods of security management and certification as providers of management and certifications. While they take different approaches, they are effective and successful insofar as they are recognized and accepted by customers depending on tastes. Therefore the GBDe has not endorsed or supported any specific model of security management and certification, but recommended that such management and certification should be operated and adopted by both governments and industries on global basis. The GBDe will continue to advocate the standardized security measures through ISO (International Organization for Standard), CERT/CC (Computer Emergency Response Team/ Coordination Center), ISAC (Information Sharing and Analysis Center), and other global conventions of both business and government. The GBDe recommends that such risk assessment and risk management should include forward-looking responses to emerging and potential threats to information systems and networks.

2. Information sharing/collaboration

The GBDe has addressed the importance of information sharing between private sectors and governmental sectors on cyber crimes since the Miami recommendations. Various international

fora have also discussed the importance of information sharing, and the US, for example, has entered the stage of real practice.

The GBDe seeks to ensure information sharing is discussed in the context of protection of information systems from the “attacks to critical infrastructure”⁸ at its initiation. In the context of reacting against terrorism and other attacks and other business disruptions, governments have already started discussions regarding the critical infrastructure at the nation’s base, and in many cases they have implemented best practices. The GBDe recommends that governments should be actively engaged in defending critical national infrastructure and cooperate with industry to ensure that measures do not cause unnecessary damage to normal business operations.

Other information sharing between public and private sectors on virus attacks or denial-of-service attacks should be discussed in a separate context from the attacks to critical infrastructures. In general, law enforcement agencies expect the owner of information systems under external attack to report any damage and request that the ISP or other private operators disclose the access logs or communication logs. Of course, such requests should be executed following due process, and special attention should be paid to avoid infringing fundamental human rights such as the protection of personal data.

The GBDe recommends that, with respect to information sharing on general cyber crimes and external attacks, both industry and governments create a reporting system that would collect all the cases found, and that industry undertake to report all the attacks. Also, each nation’s due process should be respected and care taken to ensure that individual rights are not infringed unnecessarily.

CERT/CC, ISAC, and other international fora have discussed and practiced the framework of information sharing where some of them have been achieved under the initiatives of governments, and some others have been achieved through voluntary approaches by private sectors. The GBDe will address these activities through advocacy, and promote the discussion on issues such as international cooperation and jurisdiction.

⁸ While the definition of “critical infrastructures” may differ depending on the situation, the GBDe defines that they are infrastructures including information networks which are relevant to national security and safety or have a high financial value, such as banking, finance, transportation, electric power supply, telecommunication, governmental operations, and so on.

3. Corporate Governance

Today, information and network assets are as important as financial assets for companies. Enterprises depend on their network to reach and support customers and suppliers. When a network fails to perform, costs will increase, reputations will suffer and transactions will be lost. Privacy and integrity losses may create liabilities and create costs. Maintaining a continuous business in a global, networked society is critical.

In the wake of the attacks of September 11 and CEOs' responsibility for matters of corporate management, it is increasingly important for senior management to ensure that their networks can support business continuity and profitability objectives. A trend appears to have developed toward a new form of accountability and responsibility for owners and operators of enterprise networks. In such an environment, enterprises may choose to appoint a Chief Information Security Officer (CISO) or adopt alternative measures to ensure security. Not only CEOs but also senior management should be accountable for, and recognize security management, as indispensable for corporate management.

The GBDe recommends that enterprises develop business processes for security management and establish a security management system, operated and initiated by senior management. The following items should be indispensable for global corporations and their leaders.

- A Security Policy, which clearly states the position and basic understanding of the corporation regarding information security, for example, how to protect information and data inside its own information network and system, should be established. Security Program including business continuity in emergency situation would be also effective.
- A CISO, who is responsible for information security at board level, may be appointed. He/She should be responsible for ensuring policy consistency, clearly defining policies, identifying and consistently enforcing consequences for non-compliance, and instituting a governance framework to monitor and control the execution of processes and procedures.
- Security management systems and programs should be established and operated effectively. They should be based on risk assessment and should be dynamic, encompassing all levels of corporate

activity and all aspects of corporate operations, and be initiated under the leadership of the CEO. Information system and network security policies, practices, measures and procedures should be co-oriented and integrated by security management to create a coherent system of security.

- Systems, networks and policies of corporations need to be properly designed, implemented and co-ordinated to optimize cyber security. Cyber security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. Corporations should respect and implement this principle not only as a provider of services and devices for information systems but also as an owner or operator of its own information systems and network.

4. Internet Protection

In recent years, the number of information systems damaged by hackers, viruses, and other cyber attacks has increased dramatically. To avoid and prevent damage, one possible solution for governments is to enact new laws or change existing laws. However, law enforcement can be burdensome for industries and impact on business development. Rather than place the burden on telecom corporations and ISPs to store and preserve great amounts of data and provide access to law enforcement, focusing on new or revised legislation enabling more effective education, awareness, and deterrence would be a better approach.

As mentioned above, business enterprises should recognize that cyber security is a fundamental and indispensable element of the Internet, consisting of products, services, systems and networks. From this viewpoint, their information assets are significant for management and that necessary security management should be established and enforced. The same should be true for networks of government, including local governments, and universities. For these stakeholders in cyber security, awareness should be emphasized and security policies should be created and operated by them.

The GBDe recommends that all participants and stakeholders of the Internet and e-commerce should be aware of the need for security of information systems and networks and what they can do to enhance security. Awareness of the risks and available safeguards is the first line of defense. Information systems and networks can

spread harm to others as a result of interconnectivity and interdependency. Corporations should consider such risk when establishing security policy and security management systems. All participants should also be aware of the configuration of, and available updates for, their system, its place within networks, good practices that can be implemented to enhance security, corporations should provide security information and updates to their users and consumers.

The GBDe also recommends that risk assessment of information systems and networks should be conducted and the results shared in global cases. Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to include key internal and external factors, such as technology, physical and human factors, policies and third party services with security implications. Because of the growing interconnectivity of information systems and networks, risk assessment should include consideration of the potential harm that may originate from others or be caused to others. Industries, especially major corporations, should develop such risk assessment actively on a global basis in order to establish cyber security as an indispensable element of the Internet and global electronic commerce.

5. Electronic Authentications and Digital Signature

The GBDe Cyber Security Working Group has made recommendations on digital signatures, PKI and Certification Authority relating to the interoperability of global information infrastructure in the context of cyber security. As stated in Cyber Security recommendations of the Tokyo Conference of 2001, global and interoperable certificate infrastructures should be established and be available to all people and all nations in order to protect the security of electronic commerce globally. To develop such infrastructure, many organizations, on both a regional and global basis, both by governments and industry, have developed and promoted discussion of this matter.

The GBDe will continue to engage in dialogue with other organizations on these issues, such as EESSI (European Electronic Signature Standardization Initiative), PKI Forum, Asia PKI Forum and so on. In order to develop this issue further, the GBDe recommends that the following issues should be discussed and recommended in the near future:

- Detailed issues of technology, physical and human activities, and policies should be

discussed to achieve harmonization i.e., harmonized certification policies, harmonization of accreditation and licensing criteria, etc.

- In order to promote dialogue, the GBDe should also aim to ensure an integrated approach when discussing these work streams.