



Global Business Dialogue on Electronic Commerce

Future of the Internet Cyber Security

Issue Leader (Asia/Oceania): *Shigemi Tamura*
Chairman
Tokyo Electric Power Company (TEPCO)

November, 2003

Implementing a “Culture of Security”

New issues in cyber security have been brought about by dramatic changes in the use of information systems and networks, the entire information technology environment, and the increasing interconnectivity of information systems and networks. The OECD Guidelines for the Security of Information Systems and Networks, which aim to promote a culture of security, respond to such an ever-changing environment for enhancing cyber security.

The GBDe has continued discussions on various issues of cyber security in order to support a “culture of security” from the perspectives of industries. The GBDe announced five recommendations at the Brussels Conference in October 2002, and has been discussing implementing a “culture of security” with the OECD, APEC, and government officials.

In general, the GBDe recognizes that one of the roles of industries as a part of a “culture of security” should be taking enough measures both in “business security” and “public security”. The GBDe’s focus is electronic

commerce and, most importantly, the market of goods and services furnished across e-commerce networks to consumers.

Indeed, as B2C e-commerce grows, the marketplace itself should be treated as a key infrastructure, the failure of which, through cyber security breach or otherwise, could have a material impact on commerce generally. For this reason, the notion of the scope of the “culture of security” within an enterprise extends beyond actions taken at the board, executive and management level to encompass contacts with other stakeholders, including consumers and others accessing e-commerce websites. Moreover, each industry has to play a key role in implementing cyber security of individual users in addition to the role in securing internal enterprise activities.

1. Business Security

As stated in the 2002 GBDe Brussels Recommendations, information and network assets are as important as financial assets for companies. Enterprises depend on information systems and networks as a means of reaching

and supporting customers to provide commercial goods and services. When these important means fail to perform, not only will the enterprises incur a loss, but individual users and networked society might be affected by the failures. Business enterprises should protect their own assets and keep business facilities secured by taking proper measures on all threats and vulnerabilities. These industrial efforts will help maintain a high level of cyber security for the entire Information Society.

In order to obtain sufficient internal cyber security for companies, the GBDe believes it necessary to take adequate countermeasures for all of the following aspects:

- **Executives**

As mentioned in the Brussels Recommendations, CEOs and all senior management are strongly advised to recognize security management as indispensable for corporate management and to be accountable for cyber security of their company. To achieve this objective, they should establish a coherent security policy and operate it effectively.

- **Managers of information systems and networks**

Industries, not only as providers of services and information systems but also as owners and operators of their own information systems and networks, should respect and implement a principle of “security design and implementation” of the OECD guidelines. Managers of information systems and networks fulfill their own responsibilities under appropriate instructions by executives.

- **Individual users inside company**

Individual users should use the internal information network according to the company’s security policy and guidelines. Unauthorized use should be strictly prohibited.

- **Individual users outside company**

In the electronic commerce marketplace, individual consumers are also among the stakeholders in the integrity of information systems and networks against cyber security

breaches. This integrity is one of the elements of promoting consumer confidence in e-commerce. The GBDe has already offered its Recommendations on consumer confidence and related issues, including trustmarks, digital signatures, combating harmful content and Internet payments.

This section presents our view of the mix of responsibilities which consumers and enterprises have in the B2C electronic marketplace. (Individual users also have responsibilities, discussed below, for helping to maintain cyber security which they should undertake as a part of their participation in the Information Society. We note that, while failure of B2B markets through cyber security breaches may be more damaging, participants here use proprietary technologies and define more sharply their respective duties to protect security.)

Internet service providers, and those offering goods and services in the B2C e-commerce market place, have a number of relationships with individual Internet users. For example, an e-commerce vendor may operate a number of networks systems for the display of products to Internet shoppers, the taking and processing of orders from a purchaser, payment arrangements and order fulfillment.

These multiple relationships can be defined in service contracts, click-through agreements and transactional agreements. The balance between enterprises and individuals of their respective responsibilities to protect networks may vary.

At the same time, an enterprise should treat its customers and surfing shoppers as a part of its extended zone of “business security” in order to protect against failure in the e-commerce market place. Here are some elements which e-commerce businesses should consider to foster security in the marketplace:

- Review of relationships with individual Internet users: some may be more closely tied to the business (e.g. access subscribers), while others are transitory;

- Defining the relationship on cyber security, indicating respective responsibilities, with well publicized contractual terms of use and other notices;
- Periodic reminders and updates on specific threats;
- Maintaining network security against distribution of cyber security threats to and from individuals;
- Integrating cyber security awareness into the help line/call center process (the failed transaction may be the clue to a security breach); and
- Facilitating distribution of cyber security solutions.

As a result of their dealings with consumers, service providers and vendors should consider developing codes for the purposes of standardizing practices to provide a coherent approach to cyber security issues within B2C e-commerce markets. These codes will help to manage consumers' expectations regarding the integrity of the Internet infrastructure – enhancing consumer confidence – and allow them to be active participants in building the culture of security.

If each company takes necessary and sufficient measures for cyber security as outlined above, network security will be improved. The GBDe has advocated policy recommendations in past four years regarding public/private cooperation and information sharing in many fora such as APEC and the OECD. The GBDe has contributed to the process of raising awareness of cyber security through such activities.

2. Public Security

Cyber security needs to be promoted for not only for information technology and e-commerce but also for the whole economic system of the global Information Society. The Information Society should be realized by economic development and increasing

employment from e-commerce as well as public services of e-medicine and e-education achieved by e-government. Cyber security is indispensable for these elements of the Information Society.

a. Appropriate level of cyber security

It is necessary to ensure an “appropriate level of cyber security”, which is essential to the prosperity of e-commerce and e-government, in order that the Information Society should expand and bring about social benefits globally. In order to realize such an “appropriate level of cyber security” globally, individual users, industries, and governments of Information Society should recognize the necessity of cyber security and share in its costs.

Some industries have already developed information systems and networks with enough levels of cyber security, however there are believed to be a lot of industries that do not have sufficient levels of cyber security. We should be aware that, if each stakeholder concerns him/herself too much with seeking benefits and cost reductions, investment for cyber security will be greatly reduced and information systems and network will become more vulnerable to internal and external threats.

If information systems and networks have a lower level of cyber security, damages from external attacks and internal unauthorized activities will easily occur and such damages will be passed on to other users. Individual users cannot obtain benefits from e-commerce and e-government using “unsecured” networks and information systems. If industry and government defer investment in their own information system and network security, they will expose their information assets to the danger of all kinds of threats and, even inflict unexpected damage on citizens of networked society.

b. Cost-effective security level

As written in the OECD Guidelines, industries, as well as other participants of networked society, should be accountable for the security of information systems and networks, depending upon their specific roles. Therefore,

enterprises are encouraged to decide their own security levels and invest a certain amount of money commensurate with the anticipated benefit, on the condition that they can assure the minimum security level. While enterprises can continue using open networked environments as before, with the same levels of cyber security, they also have the right to enjoy benefits from e-commerce and e-government with more secured information systems and networks, by paying much more for cyber security. This is the case not only for industries, but also individual users.

Whereas individual users can obtain secured services and facilities depending on how much they have paid, suppliers should provide hardware, software, and other services with various levels of cyber security, according to the needs of their clients. Industries, as suppliers, should help their customers to know how secured their services and machines are by appropriately providing the necessary information about cyber security.

Individual users should recognize that there is a direct correlation between the amount they have paid and the level of cyber security they receive. In cases where they require an extremely high level of cyber security, industries can isolate them from other users to provide an even higher level of security. For example, business players which own and operate critical infrastructure indispensable for civil society might be provided with an extremely high level of cyber security with entirely separated systems from open networks.

c. Relationship between industries and individual users

Individual users play an important role in maintaining cyber security. As noted above, they are often integrated into the zone of intra-enterprise security as subscribers, customers or other participants in the e-commerce marketplace. The GBDe supposes that industrial activities, including best practices, have something to do with cyber security of individual users. Of course, outside of e-commerce, individual users, as recipients of e-government services, or “netizens”, have

responsibilities to help maintain the security of the Information Society.

Individual users are obliged to comply with contracts or tariffs, which are executed for each service and facility. Through this obligation, the responsibilities of individual users of the Information Society would be guaranteed as a part of a culture of security. Industries are playing an important role to ensure the responsibility of individual users of networked society. This responsibility makes clear, and underlines the importance of, the role of industries. Industries are expected to distinguish clearly between customers and suppliers, to ensure legally the right and obligation of each stakeholder within each appropriate jurisdiction, and to publicize these rights and duties.

It is quite effective, in order to realize, for realizing an “appropriate level of cyber security”, that obligations described in contracts and tariffs stipulate the responsibilities and accountabilities of individual users. By clearly assigning the responsibilities of suppliers and users, cyber security of networked society will be clarified for individual users.

d. Standards in cyber security

As mentioned in the GBDe Brussels Recommendations of 2002, the GBDe discussed many kinds of issues regarding security standards. The GBDe did not endorse or support any specific model of security management and certification; however, it recommended that a standard model be chosen and maintained globally by the cooperative activities of governments and industries.

Considering the situation above, an “appropriate level of security” should be clarified by globally interoperable standards, and, at the same time, be promoted internationally through discussion of standardization. The GBDe supports ongoing dialogue in standardization bodies in order that an “appropriate level of security” for the Information Society be realized by objective global standards of cyber security.

Recommendations

By recognizing the important role of industries in networked societies, the GBDe makes the following recommendations in addition to those of the past four years’:

- The GBDe recommends that each government should maintain critical infrastructures and securely provide public services such as e-government while respecting individual privacy and freedom. The cyber security policy of each nation should define these governmental responsibilities.
- From the business point of view, leadership of executives is necessary for the achievement of cyber security. The GBDe supports “Information Security Assurance for Executives” by the ICC/BIAC and also continuing dialogue with ICC/BIAC and other organizations.
- The GBDe recommends that information sharing for cyber security by industry should be implemented both *upstream* and *downstream*. “Upstream information sharing” means that industry and government share incident information on attacks and denial of service on information systems and networks in order to prevent the spread of serious damages. In the process of such information sharing, “anonymity” should be guaranteed through a government agency or a specialized clearinghouse so as not to reveal the identity of the network owner/provider who was the victim of an attack or presented vulnerability. On the other hand, “downstream information sharing” means that industries should disclose indispensable information on cyber security, for example, security levels of their services, software, and hardware, and the protection measures for threats and vulnerabilities.
- The GBDe recommends that an “appropriate level of security” should be established globally in order that all people in all nations and economies could enjoy benefits from e-commerce and e-government as citizens

of the Information Society. Through dialogue and advocacy with governments, civil society, and other international business organizations, the GBDe should strive to clarify the definition of an “appropriate level of security” which should be realized globally.

- The GBDe recognizes that the security level of society will increase if enterprises define the individual user’s responsibility regarding a “culture of security”. The GBDe recommends that, when providing services and hardware regarding cyber security, industries should provide an appropriate level of security in proportion to the investments by each customer. At the same time, industries, as supply side, should make clear statements on liabilities and obligations of customers as demand side, and make sure such responsibilities will be fulfilled within their own jurisdictions. This approach should support implementing responsibilities of individual users as a part of a “culture of security”.