

GLOBAL BUSINESS DIALOGUE ON ELECTRONIC COMMERCE



CYBER SECURITY AND CYBER CRIME

SEPTEMBER 26, 2000

Issue Chair: Dick Brown
CEO
EDS Corporation

Issue Sherpa: Bill Poulos
EDS Corporation
Tel: (202) 637-6708
Fax: (202) 637-6759
email: bill.poulos@eds.com

Contact Point:
(Asia/Oceania): Dr. Hiroki Arakawa
Senior Vice President
NTT Data Corporation

Contact Point:
(Europe/Africa): Dr. Hagen Hultsch
Member of the Board
Deutsche Telekom

INTRODUCTION

Through the use of information technology, innovative applications and global networks, companies are developing new business models to create, market, distribute, and sell products and services at ever-competitive prices. Thereby, consumers enjoy increased choice and lower prices.

However, the open and interconnected nature of the Internet also involves risks and vulnerabilities. The industry sectors crucial to national and global economic stability and growth (such as telecommunications, financial services, transportation, energy, government services, and the information and communications industries) face increased threats and major economic damage when the underlying information infrastructure is targeted or made vulnerable by illegal activity.

Problems caused by recent incidents such as denial of service attacks on e-commerce sites have highlighted the need for a more resilient and secure Internet. Therefore, cyber security has become a high priority issue on the political agenda at the national, regional, and international level and with businesses all over the world. Equally important as these well publicized cyber attacks are traditional crimes committed by means of the Internet, such as theft of proprietary information and content, fraud, money laundering, and identity theft. In this paper, both traditional and new forms of offences will be addressed.

All Internet users, stakeholders, and governments must meet the security and policy challenges that an open and accessible Internet presents. The known and potential vulnerabilities raise difficult issues for businesses and governments about how to best provide protection for the world's critical information infrastructure. The infrastructure must be strengthened in order to better defend against security breaches, piracy of proprietary information and content, denial of service attacks, computer break-ins by hackers, and development and proliferation of destructive viruses that violate the confidentiality, integrity, and availability of systems by exploiting security holes or poor procedures.

Ensuring the safety and security of those who use the Internet for lawful public or private purposes is thus a critical element of electronic commerce policy that requires high priority attention by leaders in business and government. Network stability and reliability are fundamental requirements for user confidence in e-commerce technologies. Business and governments share an interest in the proliferation of an open and accessible Internet that is safe for legitimate electronic commerce transactions.

For these reasons, the GBDe is providing observations and policy recommendations to all governments, at all levels, so as to begin cooperative, international industry-to-government and government-to-government efforts to enhance cyber security and to fight cyber crime.

RECOMMENDATIONS FOR BOTH INDUSTRY AND GOVERNMENT ACTION

Global Cooperation. Cyber security and universally recognized crime must be addressed on a global Basis. Because the Internet is a global medium that does not recognize geographical, governmental, or political boundaries, the security of both public domain and proprietary information and content is an issue that must be pursued on a global basis. The nature of cyber crime and threats to the critical information infrastructure are dynamic. The security of information requires ongoing commitment, attention, and cooperation of industry and governments worldwide.

Investment in Information Assurance Services. Governments and companies should invest in information assurance and cyber security products, services, and procedures to protect the value of their business, and government information and content, and to prevent misuse by cyber criminals. All stakeholders must ensure that users can safely do business on the Internet.

Use of Existing Cyber Security Tools. The GBDe encourages continued emphasis on the use of existing security tools and the development and deployment of new security tools, authentication systems, and security processes by businesses and governments. Additionally, the GBDe strongly encourages awareness of the potential threats at all levels of government and industry as essential to security and indispensable to an effective risk management process.

R&D Funding. The GBDe recognizes that additional funding by governments for research and development will be necessary to better understand existing and future threats, and to create corresponding robust security technologies for the future. Industry normally invests in R&D that result in security products and services, while government investment is normally in longer-range efforts that lead to products for greater economic security. Joint cooperation and partnerships by universities, businesses, and government will help promote effective R&D efforts.

'Cyber Ethics.' The GBDe companies will support outreach programs designed to instill a strong code of cyber ethics among current users and in the next generation of cyber citizens. 'Cyber ethics' should become a regular and understandable part of the Internet lexicon. Security awareness and ethical on-line behavior should be taught at home, in school, and at the workplace. The implementation of education programs for 'cyber ethics' needs to be done at the individual level, in businesses, in all government organizations, and at all grade levels in schools. Safe, efficient, and legitimate on-line business operations demand the investment by schools, community groups, companies, and organizations. It is everyone's responsibility to become part of a deterrence solution, working together to establish and embrace a reasonable set of information security practices and procedures.

State-Sponsored Industrial Espionage. In order to ensure fair competition at an international level, GBDe companies oppose any state-sponsored industrial espionage to

advance the commercial interest of companies or nations. GBDe companies pledge not to accept competitive information from such sources.

Mutual Cooperation With Law Enforcement. Industry should cooperate—where appropriate and under transparent conditions—with law enforcement authorities, other authorized government agencies or relevant bodies. This also includes the sharing of information by government authorities with the private sector. Most national governments have conducted assessments of their nation’s network vulnerabilities. Governments often have collected and analyzed threat information in the process of providing for their national security. Both types of information, vulnerabilities and threats, can be of great value to businesses and governments should assess how, and to what extent, it should be shared with industry.

RECOMMENDATIONS FOR INDUSTRY ACTION

Industry Leadership in Cooperation With Governments. Businesses generally own and operate the global information infrastructure and, as such, have primary *leadership* and *responsibility* for information security requirements, standards, design, implementation, and protection. It is of vital economic interest for businesses worldwide to cooperate with all stakeholders, public and private, to provide for a secure infrastructure to ensure consumer trust.

Information Sharing While Protecting Privacy. Industry manages the private sector portion of the global information infrastructure. Industry should cooperate, company to company, in reporting and exchanging non-proprietary information concerning threats, vulnerabilities, and protective measures. Industry should also cooperate with governments in reporting attacks and incidents of cyber crime, while adhering to national law or other agreements regarding the collection, processing, and disclosure of personal data.

Information Sharing With Governments. The GBDe supports, in principal, the sharing of information, where appropriate, with representatives of governments at all levels. GBDe companies will work within national or regional efforts to identify when, how, and with whom this should occur. This must be consistent with national laws, recognizing that in most cases current laws do not address the potential liability concerns of industry resulting from information received from or provided to the government.

Mechanisms for Information Sharing. The GBDe supports and encourages businesses in all industry sectors, in all regions, to establish *mechanisms* for the systematic and protected sharing of information regarding:

- Cyber attacks
- Vulnerabilities
- Countermeasures
- Effective information security practices

The goal of information sharing mechanisms is to provide early warning and incident response to gain sufficient expertise in achieving business continuity to minimize the effect of security-related incidents on the global information infrastructure. A secondary goal is the identification and dissemination of information that could be further used by independent expert bodies in industry, academia, or government in solving technical issues, creating better security practices, or prioritizing R&D funding.

Voluntary Participation in Mechanisms. Participation in information sharing mechanisms should be voluntary, industry-led, and may be virtual, as determined by the industry stakeholders in each sector or region. It is recognized that each company must decide for itself the liability exposure it is prepared to accept for such information exchange, given the current legal structures.

GBDe Leadership in Creating Mechanisms. GBDe companies are committed to lead the development of *mechanisms* for the systematic and protected sharing of information in their respective countries. Information sharing mechanisms should be created from the initiatives of private companies and should seek to maximize global cooperation. It will be important for each mechanism to determine what information is to be shared between the enterprises or between the enterprise and the government.

Identify Barriers to Information Sharing. GBDe companies are committed to work together, with each other, with governments, and with other stakeholders to identify and, where possible, to overcome legal, structural, and competitive barriers that create disincentives to productive information sharing for the public good. The GBDe will define the nature of information sharing barriers of concern to GBDe companies and issue a progress report of our findings in 2001.

GBDe Progress Report in 2001. The GBDe will issue a progress report in 2001 to all governments regarding progress in creating such voluntary information sharing mechanisms. The objectives of the mid-year report will be to describe:

1. Where information sharing mechanisms are located around the world.
2. The make up and character of information sharing mechanisms.
3. To identify objectives of, and legal, structural, and competitive barriers to information sharing mechanisms.
4. Assess the possibility for mutual information exchange and cooperation with other information sharing mechanisms.

RECOMMENDATIONS FOR GOVERNMENT ACTION

International Agreements To Combat Cyber Crime. Any legal framework to combat cyber crime should focus on comprehensive international solutions which are carefully tailored and balanced, taking into account the expertise and adequate involvement from industry. Regulation should meet the requirements of flexibility and broad international

compatibility. Regional agreements are not sufficient to address the global nature of cyber crime.

Governments Should Clarify Substantive Criminal Laws. In order to arrest and prosecute cyber criminals, it is recommended that governments review, clarify, and make interoperable laws regarding all forms of cyber crimes, e.g., malicious hacking, cyber piracy, denial of service, and ensure that such laws are in place and vigorously enforced. This review also requires intensified cooperation in an international setting, including coordination of national law enforcement procedures.

No Increase of Regulatory Control. The GBDe encourages governments to continue to address criminal behavior on the Internet. However, governments must refrain from imposing increased regulatory control. Traditional criminal offences committed by means of the Internet should be analyzed through a policy framework that ensures that on-line conduct is treated in a manner consistent with the way offline conduct is treated.

Avoid Cost Shifting. The GBDe recognizes industry's role in assisting governments and law enforcement agencies in fighting cyber crime. However, care should be taken to not shift government costs of crime fighting directly to industry players doing business on the Internet. Government law enforcement mandates on industry must be carefully considered for their impact on costs, especially for small and medium size enterprises.

Use of Government Owned Investigative Technology. The GBDe recognizes that some national governments or law enforcement authorities are developing government owned investigative technology tools for use on-line by companies or governments for combating cyber crime. The GBDe recommends that governments and businesses cooperate and discuss the need for transparent laws and operational requirements regarding when, where, and under what conditions such tools might be used. Furthermore, as new national policies are being developed to fight cyber crime in the Internet medium, industry views should be fully considered, especially if law enforcement procedures may want to mandate companies to routinely attach government investigation technology tools to company owned and operated networks. Companies must understand the impact of such technology on a business information system and also the impact on maintaining consumer trust and privacy as well as the industry's own economic viability.

Remove Controls on Encryption. Government should remove any remaining controls on commercial encryption technologies, since encryption is a powerful tool for protection of data transmitted over the Internet or stored on computer systems. Government restrictions on the import, export, or domestic use of encryption technologies hinder security of the Internet.

Industry-led Standards to Protect Proprietary Information and Content. Many GBDe members are currently involved in ongoing multi-industry efforts to develop and deploy technical protection measures to identify and protect proprietary information and content made available over digital networks. Governments should encourage the development

and use of such industry-led measures and should refrain from mandating government requirements or standards in this area.

Government-To-Government Coordination. The GBDe strongly supports government-to-government coordination and cooperation at the international level so that law enforcement investigative demands of one country would not violate the laws of another country. This problem is expected to become more acute as the Internet makes data storage more efficient and available globally.

Shortage Of Skilled Workers. The GBDe recommends that national governments focus attention on the critical shortage of skilled workers that currently exist, especially in the information security area. The demand for security specialists will only increase as more companies are going to use digital global networks.