United States Council for International Business

1212 Avenue of the Americas, New York, NY 10036-1689
tel: 212-354-4480 ~ fax: 212-575-0327
e-mail: info@uscib.org ~ Internet: www.uscib.org

Serving American Business as U.S. Affiliate of:

International Chamber of Commerce (ICC)
International Organisation of Employers (IOE)
Business and Industry Advisory Committee (BIAC) to the OECD
ATA Carnet System

Consumer Information Security Workshop -- Comment, P024512

Submitted: Monday, April 29, 2002

The United States Council for International Business (USCIB) welcomes the opportunity to provide comments on Consumer Information Security. USCIB has been actively engaged in the revision process of the OECD Security Guidelines given our role as the U.S. affiliate of the Business and Industry Advisory Committee to the OECD. In that process, we have become even more convinced of the need for a holistic approach to security, including all participants in the information society -- business, governments, consumers, etc. Our comments will focus on this point. We are also attaching a BIAC Background note issued to the OECD in anticipation of the review Guidelines. This BIAC Background note is consistent with the comments set forth below.

The Evolution of Internet and Information Security:

The Internet has evolved from an open and relatively free, text-based network used by a handful of individuals, governments, academics and companies, into a mass communication mechanism that mixes all forms of media. Despite its evolution into a commercial as well as communications medium, the architecture of the Internet epitomizes decentralization. Moreover, the rapid growth of e-Business involves participants from all parts of society, including citizens and consumers sharing information with each other.

In contrast to the centralized and closed networks of the 1960s to early 1990s, the Internet and related online communications have rapidly established a relatively open, interconnected world. One's cyber experience is no longer limited to one's own data and files; it is potentially open to the entire world through a dial-up connection over a telephone line, a wireless link, or a high-speed connection.

Complementing and amplifying the decentralized and open character of today's information environment is the fact that computers and networks have become more capable and less expensive. The security functionality in one's hardware, operating system and desktop applications, works with an ever increasing number of security features embedded in websites and online services (e.g., online banking and stock trading). There are many security technologies in common every day use. From smart cards to encryption technology in consumer electronics, to copyright protection mechanisms for software, digital music and video, to online banking and stock trading, to secure email, to digital signatures for all sorts of online identification and data storage – demand for and availability of information security technologies and services have become all-pervasive.

It is important to recognize though, that information security is not just about encryption software or hardware. Services from consultants and e-services provided by websites, hosting services, application service providers (ASPs), online exchanges, and e-marketplaces, all touch information security in many significant ways. Corporate networks, government networks and university networks, both old and new, also significantly impact information security given the magnitude of information stored on them and transmitted over them.

Information Security Threats, Vulnerabilities and Management:

Threats: It is a critical, though usually unnoticed by many, fact that the Internet was not conceived originally with security in mind. Rather, it was designed to facilitate communication between trusted parties over a trusted network. It was not designed to preclude malicious attackers from defacing networks, stealing personal identities, or from compromising sensitive data. In hindsight, the results of this design strategy are apparent: not only can well-meaning users sometimes impair others' use of the Internet, malicious users can also periodically exploit its inherent weaknesses for financial gain, notoriety, or for the sake of political commentary.

From the "I Love You" computer virus to the cases of distributed denial of service attacks on e-commerce sites to the alteration or defacement of government websites, the threats to the security, privacy and reliability of the Internet are world wide and very significant. These threats have caused damage to stored files, computers and networks for businesses, governments and individuals, as well as resulting in inconvenience and losses of productivity and credibility. If users cannot trust the Internet and computer networks, e-commerce itself is at risk. The productivity gains and convenience of this medium may be eviscerated by the threats that exploit its very open nature. Most software and hardware companies work extremely hard to create more secure products, to identify threats and vulnerabilities, to fix problems and to deliver security solutions. Industry and government are also responding to these threats through such collaborative organizations as Information Sharing and Analysis Centers. Many popular web portals loosely collaborate on how to deal with distributed denial of service attacks. But even large sophisticated technology companies face damaging threats.

Given the relentless demand for connectivity to business partners, an attacker's possible points of entry into a network multiply exponentially. For example, stock market operators who may use the Internet to publish their market data live and in real time to their customers work with technology firms to make sure that each broker sees the latest stock price at the same time. If a hacker or virus or denial of service attack were to impact the speed or availability of such data, the functioning of the stock market is challenged.

The most significant threats to the Internet today may best be categorized according to how professional information security measures are implemented to protect against the failure of three information security services: (1) Confidentiality: Preventing undesired disclosure of information; (2) Integrity: Preventing undesired modification of information; and (3) Availability: Preventing an inability to access desired information. Threats may also be categorized proactively or reactively. Reactive categorization of threats evaluates the symptom (e.g., a tool to exploit a vulnerability) while proactive categorization searches for the underlying cause of the exploit's success.

Vulnerabilities: In contrast to threats, vulnerabilities generally are innate to systems and technology. But with the growing impact of regulation and public policy on the shape of the Internet, some are identifying the fragmented collection of rules and laws at the local, state, national and international levels as well as the custom rules governing networks and sub-networks as vulnerabilities in and of themselves. For example, export controls on strong encryption severely limited the range and strength of possible responses to the vulnerabilities for the network and conflicting rules regarding data preservation and data protection can have a similar effect. The System Administration, Networking and Security Institute, a source for vulnerability information, has issued a report identifying the top ten vulnerabilities. It is important to recognize that SANS is but one entity's view of what thinking is going on in the broad information security community.

Management: As networks become more and more interconnected and open via the Internet, new points of failure and vulnerabilities are discovered. Therefore, owners, operators and users of networks are utilizing the increasingly sophisticated tools and services available to anyone who has access to the Internet. There are many solutions varying from technological solutions to information sharing schemes. Below is a small sample of the mechanisms and technologies that enhance security:

- *Information Sharing and Analysis Centers (ISACs)* exist in the U.S. and are being created in the UK, Japan and elsewhere;

- *Computer Emergency Response Team (CERT)* is a forum that identifies security threats and vulnerabilities and reports them in a timely manner;

- *Private Sector Security Organizations (PSSOs)* such as SecurityFocus, Bugtraq and the International Chamber of Commerce's CyberCrime Unite demonstrate the pro-activity of the private sector. These PSSOs and others supplement the work occurring within technology companies to analyze their own products, to create fixes where necessary, to publish and distribute patches and to incorporate their learning into new product development. Moreover, technology companies regularly collaborate informally to share information about potential threats;

- *Technology tools* are well known and include:
  -various encryption methods
  -firewalls,
  -anti-virus software,
  -automatic software updates for seamless security patch delivery
  -network traffic management and intrusion detection systems; and
  -access, authorization and authentication controls from basic passcode protection to biometrics and PKI solutions.

A Holistic Approach to Information Security:

This may seem obvious given the inter-connected nature of the Internet and the networked environment, but it is absolutely critical to highlight that any attempt to completely divide the world of information security into an industry zone a government zone or a consumer/user zone is antithetical to the inter-networked culture of modern computer driven communications. Indeed, the networked nature of the economy means that the entire value chain, including the end user, must be engaged in thinking and acting to assist in a secure infrastructure.

Security requires a holistic approach with each participant undertaking measures appropriate to their role, understanding that there may be principal spheres of influence and that collaboration on many levels will be required.

Greater outreach is needed to raise awareness and more education is required on a broad range of topics from software implementation and use, to password maintenance and control, to dissemination of information on new authentication, encryption and intrusion detection technologies. Every participant must exercise due diligence and act responsively. In fact, the revision of the OECD Security Guidelines is focusing on the development of a Culture of Security, whereby all participants in the networked world understand that they have a role to play in enhancing security and that their actions can have an effect well beyond their own sphere of influence. Thus, the revision process of the OECD Guidelines has highlighted the need for such a holistic approach.

As indicated above, a holistic approach recognizes that different participants may have principal spheres of influence. Below is a short analysis of these principal spheres among the three major participants -- governments, business and consumers/users.

A Role for Government: A primary role for government is to help raise awareness and to educate all stakeholders. We strongly encourage governments to work together to improve how they help promote security in the developing world. Moreover, Governments must ensure that, as network operators, they engage in effective security risk assessment and risk management. As a general principle, and specifically in the area of security technologies, government should take a limited, supportive and enabling role in the development of commercial standards, which should emerge from the globally recognized voluntary, industry led, market driven standards process. This is no less true of such sensitive security technology areas as Public Key Infrastructures than for electrical power requirements and network connectivity protocols. Moreover, the role of government-as-customer can not replace, and should not dictate, the voluntary standards process. Inherent in the concept of proportionality is the need to assure that the administrative burdens of record keeping and compliance do not result in unintended consequences that impede the use or deployment of security technology.

A Primary Role for Business: A primary role for business is to continue to develop and deploy security solutions to constantly changing threats and vulnerabilities that reflect effective security risk assessment and risk management. This includes effective and appropriate training of employees. Moreover, industry should continue to share information regarding security threats, as appropriate in the furtherance of security. In the context of viruses, they are so common now that many information security professionals are usually able to find fixes or other remedies within minutes, hours or a day. Such rapid response results, in part, from the open nature of the industry collaboration. And because the collaboration remains unfettered, the resiliency of industry remains strong.

A Primary Role for Consumers: A primary role for consumers is to ensure that they understand the security risks of the networked environment and to undertake measures that limit the potential security risks that they confront.

Finally, all parties, government, industry and consumers alike, must be cognizant that the market for security products and services is dynamic, innovative and growing with great speed. Government intrusion will stop

this growth through burdensome, unintended consequences that stifle business and needlessly limit personal freedoms. These burdens may be in the form of actual regulatory compliance obligations or may be the result of reporting or other administrative requirements. Lastly, these burdens are not always readily apparent to policy makers in terms of sheer volume, potential overhead and compliance costs. Recognizing and minimizing these potential burdens is one of the major reasons for ensuring broad consultation with industry in the development of government policy.

Conclusion:

The major objective of this comment to stress that all participants in the networked world understand that they have a role to play in enhancing information security. Though particular participants may have principal spheres of influence, each participant must act responsibly so as to promote security. Industry looks forward to continuing to work with governments to promote this holistic approach to security, in furtherance of a culture of security.