CYBER SECURITY INDUSTRY ALLIANCE

CyberSecurity
A Global Challenge

In recent years, the world has witnessed a series of shocking events. Terror attacks in Bali, Madrid, London, and New York have focused international attention on physical security issues. Threats to cyber security bring a virtual dimension to the task of protecting vulnerable infrastructures. This is especially true as technology integrates more deeply not only with daily life, business, and finance, but national defense systems.

Cyber attacks and security breaches cost world economies billions of dollars of direct losses. Stolen identities can shatter innocent lives; stolen intellectual property can ruin businesses or foil military plans. Damaged or stopped systems, furthermore, can interrupt critical services.

Cyber security increases accountability, ensuring the integrity of data and financial databases. Cyber security may include technology, policies, and training to achieve its goal of protecting and assuring information quality. In this context, the Cyber Security Industry Alliance (CSIA) actively pursues a global agenda aimed to:

- raise the profile of cyber security;
- promote information sharing, threat analysis, and contingency planning;
- encourage research and development as well as security education.

As the only association focused exclusively on cyber security public policy, CSIA takes a leadership role in bringing the private sector together with international, federal, and state governments to highlight policy issues associated with cyber security worldwide. In addition to the issues below, CSIA seeks to build relationships with the European Network Information Security Agency (ENISA) and other authorities in Europe to develop a more global agenda centered on initiatives such as i2010.

Educate Policy Makers

Knowledge about IT security policy among lawmakers and government officials in world capitals is limited. This affects the quality and efficacy of IT security legislation. An important aspect of the Cyber Security Industry Alliance mission, therefore, is the education of policy makers worldwide.

Recent breaches of security at investment brokers, universities, and other large data bases filled with personal information, for example, have resulted in calls for regulating the storage and processing of personally identifying information. Members of the Cyber Security Industry Alliance have extensive experience creating solutions for the many technical security

Developing a series of cyber security policy initiatives for businesses and firms that operate on a global scale requires not only non-partisan government leadership and international coordination, but direction from the private sector as well. The Cyber Security Industry Alliance—a public policy and advocacy group of security software, hardware, and service vendors worldwide—welcomes new CSIA members and their input to helping shape these necessary initiatives.

safeguards and best practices needed to protect consumer privacy, reduce identity theft, and ensure the safe keeping of individually identifiable information.

CSIA has lobbied for the establishment of national policies built in conjunction with the private sector. It has also sought to establish a framework for protection by denoting key areas of risk, security solution requirements, and best practices. With these goals in mind, CSIA recommends that Congress:

- Take a comprehensive approach to addressing cyber security issues. Currently, Congress is considering cyber security problems such as spyware, phishing, and data warehouse security on an individual basis. CSIA believes that understanding information security issues with a broad perspective will provide a solid foundation for successful policymaking.
- Support federal preemption of the multitude of breach notification laws being passed in State legislatures.
- Advocate Senate ratification of the Council of Europe's Convention on Cybercrime, which assures the public that appropriate resources will be available to prosecute cyber-criminals on a global basis.
- Investigate tax benefits and similar incentives to encourage businesses to implement stronger cyber security measures.

In addition to educating lawmakers about cyber security issues, CSIA believes it is also imperative to teach children with regard to cyber security and cyber ethics. As a public service, members of the Cyber Security Industry Alliance fund educational efforts and initiatives for promoting cyber security awareness among children and for leveraging partnerships between parents and teachers to that end.

What is vulnerable to attack

- Personal information
- Business information
- Critical infrastructure systems
- Government systems

Ratifying the International Convention on Cyber Crime

Cyber crime poses a huge threat to global society. Transcending geographical and national borders, cyber crime is also challenging existing legal concepts, as cyber criminals are often in places other than where their crime hits victims.

The Council of Europe's International Convention on Cyber Crime is the first and only multilateral treaty addressing the need for cooperation in the investigation and prosecution of computer crimes. It includes, for instance, provisions for traditional and computer crime related mutual assistance and extradition rules.

To become effective, the Convention on Cyber Crime requires ratification by five countries, at least three of whom are in the Council of Europe. Those conditions were met and the Convention entered into force on July 1, 2004. As of August 1, 2004, Council of Europe members who have ratified the Convention include Albania, Croatia, Estonia, Hungary, Lithuania, and Romania. There are 28 other members of the Council of Europe and 4 non-member countries, including the United States, who have not ratified the Convention.

CSIA believes it is important for the U.S. Senate to quickly consider and ratify the Convention on Cyber Crime and has lobbied on the Convention's behalf. Ratification by the U.S., CSIA argues, requires no new legislation, removes or minimizes legal obstacles, denies safe havens to cyber criminals, and safeguards civil liberties.

For additional information :
http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Guide Corporate Governance

Worldwide, there are many pieces of legislation with international implications regarding IT security, from European Union Privacy Directives to such US legislation as the 2002 Sarbanes-Oxley Act. The latter, named after its sponsors in Congress, requires senior management of publicly traded companies to be personally responsible for establishing and maintaining adequate internal controls for financial reporting. It also requires annual assessment of the effectiveness of those controls.

Defining the obligations of publicly traded companies in securing those IT systems essential for the integrity of financial reporting has since engendered considerable discussion and debate.

The Cyber Security Industry Alliance recognizes that, given the size and complexity of IT systems in most publicly traded companies, the statutory and administrative materials governing this aspect of Sarbanes-Oxley may be unclear. Managers need more specificity regarding IT governance to guide and inform their compliance efforts. Consequently, CSIA called for a national summit of senior managers, auditors, and IT professionals to explore such issues.

Conducted in the spring of 2005, the CSIA "Sarbanes-Oxley" Summit considered how various parts of the law—statutory, regulatory, and administrative—connect with regard to information security. Participants gained a better understanding of how information security requirements are part of the law's compliance. In addition, participants received assistance in developing appropriate IT security strategies.

Monitoring and influencing legislation and government regulation is an integral part of the Cyber Security Industry Alliance mission. As with the Sarbanes-Oxley Act of 2002, CSIA gives member companies a platform from which they can exert their expertise and advice to help ensure that decisions in world capitals—from the European Union to Washington—do not adversely impact business.

Monitor Emerging Technologies

Information systems are not static. Industry and government are rapidly deploying new technologies ranging from Voice over Internet Protocol (VoIP), Radio Frequency Identification (RFID) Tags, and advanced wireless cellular systems such as "WiMax." Each of these areas prompts new issues about security and reliability of information systems. The Cyber Security Industry Alliance helps ensure each of these technologies is deployed as widely as possible while ensuring security, privacy, and availability.

Recently, CSIA co-hosted a workshop entitled "On Securing Voice over IP: Harmonizing Technology and Policy." Conducted in Washington D.C. June 1 and 2, 2005, the workshop gathered an international group of scientists, technologists, policy makers, and domain experts to facilitate constructive discussion on new policy considerations regarding VoIP security.

Experts believe VoIP, technology that allows phone calls to move in packets over the public Internet rather than traditional private telephony circuits, will transform the telecommunications industry. Commercial use is rising because IP telephony is typically more economical than traditional telephone service. Moreover, IP telephony usage will soar when customers adopt WiFi cell phones, and may become ubiquitous when

What is cyber security

Cyber security is the protection of:

- computers
- electronic communications systems
- electronic communication services
- wire communication
- electronic communication

CSIA Membership benefits industry, business

CSIA Action:	Examine cyber security implications of regulatory legislation coming out of Washington, Brussels, and other governments.
Member Benefit:	Serve global business customers from a stronger international position.
CSIA Action:	Improve the Common Criteria process.
Member Benefit:	Improve the product certification process; assist in investigating potential commercial use of Common Criteria products.
CSIA Action:	Increase understanding of cyber security policy issues in key government capitals.
Member Benefit:	Help ensure that decisions in world capitals do not adversely impact business.
CSIA Action:	Advocate adoption and ratification of the Council of Europe's International Convention on Cyber Crime.
Member Benefit:	Streamline legal procedures and lower legal costs.
CSIA Action:	Prepare a cyber security R&D agenda to summarize the current state of global cyber security funding, and develop a list of priorities for governments to fund over the next ten years.
Member Benefit:	Maximize return on R&D investments while influencing longer term development.

wide area wireless technologies such as WiMax are commonplace.

The Achilles heel, however, is cyber security. Since IP telephony depends on the Internet, VoIP is subject to all cyber vulnerabilities on the Internet. In fact, VoIP multiplies the impact of Internet-borne attacks because the architecture for an IP telephony system also offers many points of vulnerability. Potential targets include IP phones, broadband modems, gateways for signaling and media, soft switches, and servers for IP telephony applications. Standard cyber security equipment and applications often do not protect IP telephony because VoIP security demands an extra measure of processing capability.

Potential fallout from cyber attacks

- ■ Slowed systems reduce productivity
- ■ Erased, stolen, or corrupted data trigger financial or strategic loss
- ■ Damaged or stopped systems interrupt critical services

Repercussions can have a crippling impact on the information technology underpinning critical infrastructures such as banking and finance, chemical, civil defense, electrical power generation, oil and gas production, and transportation systems. While CSIA member companies advocate the wide deployment of VoIP and other emerging technologies, they also work to protect the entire information technology ecosphere.

Strengthen International Standards

CSIA supports broad use of a single efficient and effective process for security certification. Presently, competing international standards create compliance problems when applied to the product certification process. Different countries are developing different guides for implementing the international information technology security standards called Common Criteria. As a result, there is no clear measure for assessing the value of product certification to end users.

For example, the National Information Assurance Partnership (NIAP) is a U.S. government initiative to meet cyber security testing needs of consumers and producers of information technology. NIAP also oversees U.S. implementation of the Common Criteria. The intention of NIAP is to increase the level of trust in IT systems and networks with cost-effective security testing, evaluation, and validation programs that conform to accepted international standards. Many commercial users, however, are concerned that because NIAP testing has mainly served government agencies in the U.S. defense and intelligence communities, it may prove ineffective, unrealistic, or cost prohibitive for their needs. CSIA wants to improve the Common Criteria and NIAP process to achieve the promises of NIAP certification and to avoid the pitfalls of a balkanized certification environment. Beginning with a Common Criteria Users' Forum, held in the Washington D.C. area October 2004, CSIA has sought to leverage the process to 1) address both private sector and government needs; 2) foster broader input from users and the industry; and 3) ensure that federal procurement policy related to NIAP certification is understood and consistently applied.

Governments have invested millions of tax dollars to develop the Common Criteria. CSIA believes the idea of NIAP-authorized certification, based on Common Criteria security standards, is crucial for helping the IT industry improve cyber security and protect critical infrastructure. ■

Create opportunities

Launched in February 2004, the Cyber Security Industry Alliance shapes cyber security policy through public policy initiatives, public sector partnerships, corporate outreach, academic programs, alignment behind emerging industry technology standards, and public education. CSIA creates opportunities for member companies to influence policy decisions worldwide, directly impacting business and the industry.

For a list of member companies, press releases, white papers, and membership information, contact:

Cyber Security Industry Alliance
2020 N. 14th Street
Suite 750
Arlington, Virginia 22201
U.S.A.
Tel: +1 703 894 2742
www.csialliance.org