CYBER SECURITY INDUSTRY ALLIANCE

Information, Influence

privacy, reliability, integrity

year in review 2005

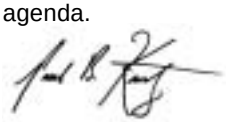
Much Accomplished, Much To Do

The Cyber Security Industry Alliance was formed in 2004 with clearly stated objectives: Monitor and influence public policy; Develop and build awareness campaigns; Identify, support emerging technology standards. Our goal is the same now as then, to ensure the privacy, reliability, and integrity of information systems. Success depends on the combined strength of our individual members.

We are pleased with our progress. In 2005, CSIA tracked nearly 40 bills and actively engaged Congressional staff on more than half of them relating to data breach notification, health care, and telecom reform. Among our accomplishments:

- CSIA improved its profile in Congress, testifying three times before committees in both chambers. We also sponsored briefings for members of Congress and their staff on cyber security issues including spyware and digital control systems.
- CSIA efforts regarding data breach notification legislation led to the inclusion of specific language within the House Commerce Committee bill affirming encryption as a best practice; CSIA influenced language within the Energy Policy Act of 2005 includes provisions to secure the Nation's power grid.
- CSIA efforts helped prompt the Senate Foreign Relations Committee to favorably review the Council of Europe's Convention on Cybercrime and to request ratification by the Senate as soon as possible.

There is much work to be done still. Creating a secure online environment can only be achieved through a comprehensive effort involving the implementation of appropriate public policy, effective security technology, high industry standards, and support from governments worldwide. As our "2005, Year in Review" testifies, this has been our agenda.



Paul Kurtz, CSIA Executive Director

Raising Awareness

CSIA advocacy efforts substantially raised the profile of cyber security in 2005, influencing congressional legislation, establishing relationships within the European Union, and educating the public in general. Testimony before the House Homeland Security Committee, for instance, led to the first dedicated cyber security post within the federal government's Executive Branch.

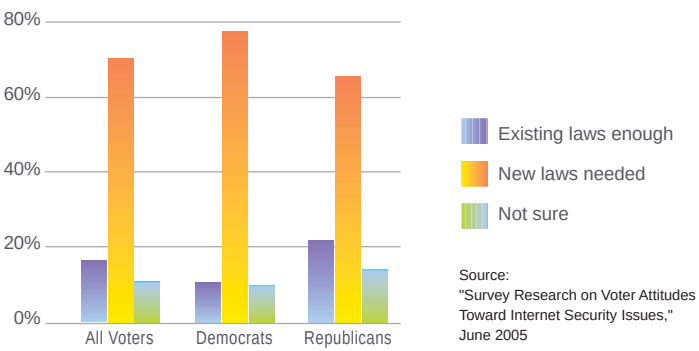
Also, a CSIA-commissioned survey this year shows voters, Republican and Democrat, expect the government to play a greater role in protecting consumer privacy on the Internet. Nearly half, in fact, say they avoid making online purchases because they are afraid their financial information may be stolen. To address such concerns, CSIA sponsored briefings for members of Congress and their staffs covering a wide range of cyber security issues, from spyware and phishing to Internet Protocol telephony.

Overseas, CSIA is beginning to raise the profile of cyber security within the European Union, building relationships with the European Network Information Security Agency (ENISA), the Council of Europe, and other authorities.

2005 was a busy year for the Cyber Security Industry Alliance, but the hard work is just beginning. Much remains to be done.

Government Needs to Do More

Do voters think existing laws are enough to protect consumer privacy on the Internet, or do they think new laws need to be written?



Source:
"Survey Research on Voter Attitudes Toward Internet Security Issues," June 2005

Demonstrating Leadership

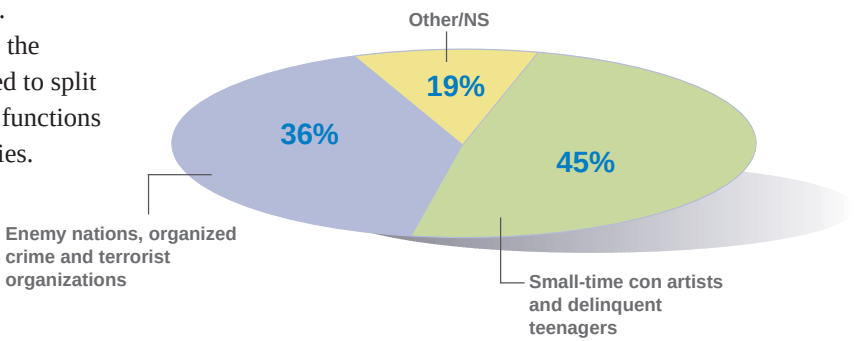
The United States cannot build a strong cyber security policy without strong leadership. That's why CSIA exercised its own leadership in leading the fight for a dedicated cyber security post at the federal government's Executive Branch level.

Testifying before the House Homeland Security Committee in April, CSIA called attention to the fact that the Department of Homeland Security had no senior leadership dedicated to cyber security needs. The absence of a dedicated cyber security chief, CSIA argued, put our information infrastructure needlessly at risk.

With support from CSIA, the House of Representatives moved to split the physical and cyber security functions between two Assistant Secretaries. These efforts were rewarded in July, when DHS Secretary Chertoff announced the department was creating the position of Assistant Secretary for Cyber Security and Telecommunications.

With the resources and authority to effectively direct public-private efforts to harden our nation's IT and communications infrastructure, the new position is a significant first step in preparing for, protecting against, and recovering from cyber attacks.

Biggest Threats to the Internet



Source:
"Survey Research on Voter Attitudes Toward Internet Security Issues," June 2005

Congressional Involvement

CSIA is the dedicated voice for cyber security on Capital Hill. We take this responsibility seriously, as the success of our 2005 agenda demonstrates. This year, CSIA has participated in the preparation of principals for cyber security legislation; provided expert comment on draft legislation; and issued documents, letters, and reports advocating public policy initiatives.

Capital Hill meetings and briefings have involved key congressional committees, including House Committees for Energy and Commerce, Government Reform, Homeland Security, and the Veterans Affairs Subcommittee on Oversight & Investigation. In the U.S. Senate, CSIA engaged the Commerce and Judiciary Committees as well as the Republican High Tech Task Force.

Thanks in part to CSIA advocacy, leading lawmakers recognize cyber security as a matter of national and economic security, critical to protecting our country's infrastructure, ensuring the continuity of operations, and maintaining emergency communications.

Congress Hears Our Voice

In 2005, CSIA tracked nearly 40 bills and actively engaged Congressional staff on more than half of them. Cyber security issues involved data breach notification, spyware, health care, and telecom reform.

Here are some accomplishments:

- **CSIA efforts regarding data breach notification legislation led to specific language within the House Commerce Committee bill on affirming encryption as a best practice.**
- **CSIA efforts helped prompt the Senate Foreign Relations Committee to favorably review the Council of Europe's Convention on Cybercrime and to request ratification by the Senate as soon as possible.**
- **CSIA efforts helped ensure the Energy Policy Act of 2005 included provisions to secure the information infrastructure of our nation's power grid.**

Building a Global Perspective

It is our job to be heard in Washington; it is also our job to be heard in Brussels. This year, CSIA joined with European Union corporate, political, and technology leaders to learn more about Europe's legal system as it pertains to cyber security issues, and to promote a global dialogue on the convergence of cyber security legislation.

As witnessed in laws like Sarbanes-Oxley, Gramm-Leach-Bliley, and the European Union's e-Privacy Directive, there are distinct differences in the way cyber security is treated on either side of the Atlantic. From a regulatory perspective, Europe has essentially taken a top-down approach to privacy and data protection. For example, the EU's Data Protection Directives, which span all sectors of the economy, tend to be more comprehensive and specific than U.S. laws relating to data retention and securing sensitive information.

The U.S. takes a more bottom-up approach to data protection and privacy, and tends to be more reactive to emerging threats on a sector-specific basis. Legislation coming from both sides of the Atlantic impacts how corporations conduct international business. In coming months, CSIA will consult with policy makers from both systems to ensure that conflicting regulations do not hold back the global economy.

Legislation coming from both sides of the Atlantic impacts how corporations conduct international business.

Policing Cybercrime

CSIA heads a coalition of twelve industry associations in the fight against cybercrime. Members include Business Software Alliance, the Business Roundtable, and the Financial Services Roundtable. The coalition's objective: Ratify the Council of Europe's Convention on Cybercrime, the first and only international treaty aimed to protect society from computer related crime.

In recent years, fast-moving computer viruses have disrupted business operations and emergency services worldwide. Corresponding losses have cost Americans billions of dollars. Because it transcends geographical and national boundaries, cybercrime challenges existing legal concepts.

The Council of Europe engineered the Cybercrime Convention to resolve these legal issues and promote a common, cooperative approach to prosecuting people who commit cybercrime. The convention defines use of terms; provides a framework of measures for implementation by sovereign states; and includes provisions for traditional and computer crime-related mutual assistance and extradition rules.

CSIA leads the fight for ratification

Here's why:

- **Ratification demonstrates U.S. leadership and requires no new legislation.**
- **Ratification removes or minimizes legal obstacles to international cooperation that currently impede U.S. investigations and prosecution of cybercrime.**
- **The Convention denies safe havens to cybercriminals.**
- **The Convention safeguards civil liberties, i.e. ratification will protect the privacy and civil liberties of Americans from efforts by foreign powers to investigate or prosecute incidents of alleged cybercrime based on political or religious motivation.**

Research & Development

Federal leadership in cyber security R&D is lacking. Funding at critical institutions such as the National Science Foundation and the Department of Homeland Security has been well below levels authorized in the Cyber Security Research and Development Act of 2003. Consequences could be catastrophic if the situation is not reversed.

In July of this year, CSIA outlined a ten-year federal funding plan for cyber security R&D. CSIA's plan prioritizes the federal R&D agenda along lines recommended earlier by the President's Information Technology Advisory Committee (PITAC).

CSIA stepped up to the plate, advancing PITAC's R&D agenda after the committee was dissolved in June. Its report, entitled "Federal Funding for Cyber Security R&D," takes note that the Internet—once a DARPA (Defense Advanced Research Projects Agency) experiment—launched a technology revolution, produced jobs, increased productivity, and provided a higher standard of living. Such dramatic consequences would not have taken place without federal funding for R&D early on.

CSIA plans to work closely with the newly designated Assistant Secretary for Cyber Security and Telecommunications at the Department of Homeland Security to jumpstart federal funding for cyber security and create, in the process, a national vision for cyber security R&D.

Information, Education

CSIA understands the media is a critical player in the public policy process. CSIA's active cyber security PR program resulted in more than 150 media mentions in the year 2005, including print, radio, and television.

CSIA Informs Congress

Whitepapers, prepared by industry experts and forwarded to critical legislators, also raise cyber security awareness. As the 109th Congress enters its 2nd session, CSIA will continue to advocate for stronger cyber security through whitepapers such as:

- **Policy Considerations for Securing Electronic Data**
- **Survey Research on Voter Attitudes Toward Internet Security Issues**
- **Cyber Security for IP Telephony**
- **Making Telework a Federal Priority: Security is Not the Issue**
- **Federal Funding for Cyber Security R&D**
- **National Agenda for Government Action on Information Security**

The public needs to know how cyber security affects them; Congress needs to know public concerns; Industry needs to help Congress address the public's concerns. CSIA—through our newsletters, press coverage, and industry summits—ensures this circle of communication is not broken.

For example, the June 2005 CSIA-commissioned survey on "Voter Attitudes Toward Internet Security Issues" shows voters are looking to Congress for leadership with regard to cyber security problems. In August, a CSIA-sponsored conference reached similar conclusions: Industry compliance under Sarbanes-Oxley has been poorly understood by corporate America. This, in part, is because Congress has been silent on the issue of IT, and CEOs listen and act on what Congress says.

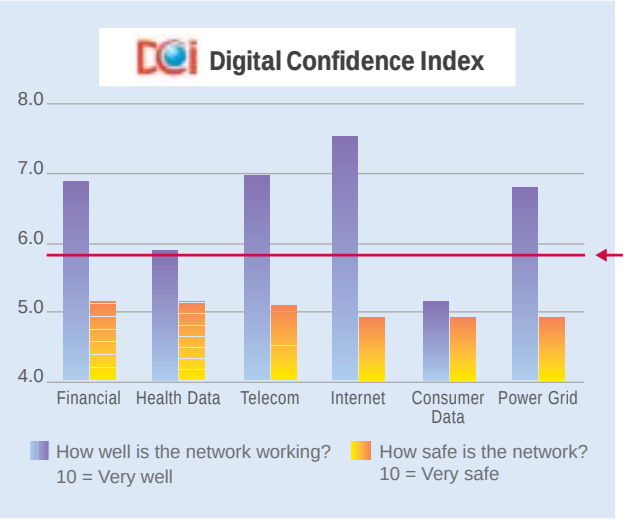
As corporate America and the public become more attuned to cyber security, congress will increasingly look to CSIA for technical guidance.

The Road Ahead

These are still the early days of e-commerce, yet online consumer spending in the United States grew 26% last year to surpass a record level $117 billion. Likewise, commercial use of Voice over Internet Protocol (VoIP), already on the rise, is expected to soar with implementation of advanced wireless cellular systems.

New technology brings new challenges, however, as serious data breaches demonstrated this year. IP telephony, moreover, is as vulnerable to cyber attacks as the Internet itself. Security breaches cost world economies billions of dollars each year while malicious spyware, phishing attacks, and related Internet fraud steal personal identities, rob bank accounts, and threaten intellectual properties on a daily basis.

The fight for cyber security is just beginning. As the Cyber Security Industry Alliance looks to the new year ahead, it will continue to work with partners at home and abroad to protect our nation's financial stability; harden the Internet economy and create a 'safer place' for business; and to accelerate security technologies that may not otherwise be funded in an industry-only setting.



Low confidence in the nation's digital infrastructure indicates need for improvement.

Source:
CSIA & Pineda Consulting

CSIA is the only association focused exclusively on cyber security public policy, bringing the leaders in IT Security together with international, federal, and state governments.

CSIA Membership includes the following companies:

Application Security, Inc.
BindView Corporation (NASDAQ: BVEW)
Check Point Software Technologies Ltd. (NASDAQ: CHKP)
Citadel Security Software Inc. (NASDAQ: CDSS)
Citrix Systems, Inc. (NASDAQ: CTXS)
Computer Associates International, Inc. (NYSE: CA)
Entrust, Inc. (NASDAQ: ENTU)
Internet Security Systems Inc. (NASDAQ: ISSX)
iPass Inc. (NASDAQ: IPAS)
Juniper Networks, Inc. (NASDAQ: JNPR)
McAfee, Inc. (NYSE: MFE)
PGP Corporation
Qualys, Inc.
RSA Security Inc. (NASDAQ: RSAS)
Secure Computing Corporation (NASDAQ: SCUR)
Surety, Inc.
Symantec Corporation (NASDAQ: SYMC)
TechGuard Security, LLC
Visa International
Vontu, Inc.

About the Cyber Security Industry Alliance

CSIA is the only advocacy group dedicated to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education and awareness. The organization is led by CEOs from the world's top security providers, who offer the technical expertise, depth and focus to encourage a better understanding of security issues. It is the belief of the CSIA that a comprehensive approach to ensuring the security of information systems is fundamental to global protection and economic stability.

To learn more about the CSIA, please visit our Web site at **www.csialliance.org** or call: **+1-703-894-2742**