

**Testimony of Harris N. Miller
President, Information Technology Association of America (ITAA)**

**Before the
Senate Committee on Commerce, Science and Transportation
Subcommittee on Science, Technology and Space**

“Internet Security”

July 16, 2001

Introduction

Chairman Wyden and Members of the Subcommittee, thank you for inviting me here to testify today on Internet security. My name is Harris N. Miller, and I am President of the [Information Technology Association of America](#) (ITAA), now celebrating its 40th Anniversary. I am proud that ITAA has emerged as the leading association on cyber security issues. ITAA represents over 500 corporate members. These are companies that have a vested economic interest in assuring that the public feels safe in cyberspace; in the United States and around the world, the vast majority of the Internet related infrastructure is owned and operated by the private sector.

I am also President of the [World Information Technology and Services Alliance](#) (WITSA), a consortium of 41 global IT associations from economies around the world, so I offer a global perspective. ITAA also houses the [Global Internet Project](#) (GIP), an international group of senior executives that are committed to fostering continued growth of the Internet, and which is spearheading an effort to engage the private sector and governments globally on the Next Generation Internet and related security and reliability issues. The GIP recently sponsored a major event on security and privacy in the next generation of the Internet that drew industry leaders from around the world.

I commend this Subcommittee for holding today’s hearing on Internet security, and I submit to you that security is ultimately a business challenge that must be addressed at the highest levels of corporate hierarchy. Customers and citizens – whether consumers in the B2C space, or business partners in B2B operations, or Americans receiving services electronically from their governments – demand it.

The stakes involved are enormous. Information technology represents over 6 percent of global gross domestic product (GDP), a spending volume of more than \$1.8 trillion, and over 8 percent of US GDP, according to [Digital Planet 2000](#), a report released last year by WITSA. According to the [US Department of Commerce](#), IT accounted for approximately one-third of the nation’s real economic growth from 1995 to 1999. Despite the current slowdown, IT-driven productivity increases have enabled our country to have what many economists thought we could not have: high growth, low unemployment, low inflation, and growth in real wages.

The IT industry's importance to the economy goes beyond the numbers I just recited, however, because the IT industry is not only a vertical industry—such as financial services or health care—it is also a horizontal industry whose technology and services under gird all the other industry sectors. For instance, the failure of a particular IT company to meet the information security challenge not only hurts that company's bottom line, it also hurts the bottom line of companies to which it provides software or IT services.

The Evolution of the Internet

In order to look at security issues surrounding the Internet, we need to first recall its intended nature. The Internet, when it was created nearly thirty years ago, was a collaborative product developed by industry, government and academia. It was designed to be an open, borderless medium for communication and sharing information, and was not programmed with security features. Nor was it intended for commercial use.

As they say, we've come a long way, baby. As you know, the Internet today is used extensively as a commercial medium, augmenting or even forming the basis of entire business models. Forrester research estimates that worldwide B-to-C e-Commerce revenues will reach \$96 billion this year. According to a report by eMarketer, B-to-B online commerce revenues will nearly double this year to reach \$448 billion, with fifty-seven percent of that commercial activity occurring here in the U.S.

And we are moving forward still. Quickly. Most Internet executives will tell you that in the not too distant future, we will live in a truly digital world, transformed by Internet technology. The Internet will be ubiquitous, seamless and integrated into everything we do. Digital ubiquity means that we no longer consciously think about how we use and access information on the Internet. Phrases like "always on" and "24/7" will be quaint. Just as we assume that the power grid is always available, we will have Internet Protocol in and on everything – our cars, our home appliances, even the products we buy at the supermarket. The Internet will allow these items to communicate – forming a virtual information bubble around our lives, anticipating and addressing many of our needs.

Mobile or Ubiquitous Commerce will be enabled by wireless networking. Individuals will move from network to network through the use of mobile computing, becoming guests on others' networks. This is already starting to happen around the globe.

The growing e-commerce space and the very real prospect of digital ubiquity pose challenges in securing the Internet. Government and businesses increasingly have as much at stake digitally as physically. Assets and value are no longer based on material objects but on information, knowledge and network connections. In the old economy and the new, more businesses are using technology to manage operations, sales, employee relations, partnerships and supply chains. More revenue is derived and more cost savings realized from online activity.

Yet the same companies and organizations that devote considerable financial and human resources to physical security pay much less attention—or, sometimes, virtually no attention—to cybersecurity. Just like a business cannot properly function without sound financial processes and systems, the same has become true for managing network activity and the valuable, critical information that flows through the network.

As I mentioned earlier, the Internet was not designed with commercial and security features in mind, yet as businesses become dependent on it for growth and market share, vast security needs have emerged. ITAA believes strongly that for this reason, Internet security measures must be addressed at the CEO and boardroom level of every company and by political leadership at all levels. And this attention must occur around the globe, not just in the U. S.

Economy at Risk

Cyber crime places the digital economy at risk. Just as the reality or threat of real crime can drain the economic vitality of neighborhoods, cities and even nations, so to can the reality or threat of crimes committed online against people and property shutter businesses and cause an otherwise motivated digital public to break their Internet connection.

Cyber crime falls into several categories. Most incidents are intended to disrupt or annoy computer users in some fashion. Distributed denial of service (DoS) attacks crash servers and bring down websites through the concerted targeting of thousands of email messages to specific electronic mailboxes. Viruses and other malicious code introduce phantom computer software programs to computers, designed intentionally to corrupt files and data. Other online intrusions are conducted to deface websites, post political messages or taunt particular groups or institutions. Even though no one stands to profit, damages caused by such attacks can run from the trifling to the millions of dollars. What motivates these attackers? Hackers may view the attack as a technology challenge, may be seeking to strike a blow against the establishment, may be looking for group acceptance from fellow hackers, or may be just indulging themselves in a perverse thrill.

Other cyber criminals are more material guys and gals. They hope to profit from their intrusions by stealing valuable or sensitive information, including credit card numbers, social security numbers, even entire identities. Targets of opportunity also include trade secrets and proprietary information, medical records, and financial transactions.

For some cyber criminals, the Internet is a channel for the dissemination of child pornography and a tool used in the furtherance of other crimes against children and adults. These crimes include fraud, racketeering, gambling, drug trafficking, money laundering, child molesting, kidnapping and more.

Cyber terrorists may seek to use the Internet as a means of attacking elements of the physical infrastructure, like power stations or airports. As we have seen in the Middle

East, cyber terrorists encouraging political strife and national conflict can quickly turn the Internet into a tool to set one group against another and to disrupt society generally.

Another class of cyber criminal and, unfortunately, the most common is the insider who breaks into systems to eavesdrop, to tamper, perhaps even to hijack corporate IT assets for personal use. These could be employees seeking revenge for perceived workplace slights, stalking fellow employees, looking for the esteem of peers by unauthorized “testing” of corporate security, or other misguided individuals.

Regardless of category, the threat is real. [A recent study](#) produced by Asta Networks and the University of California San Diego monitored a tiny fraction of the addressable Internet space and found almost 13,000 DoS attacks launched against over 5000 targets in just one week. While most targets were attacked only a few times, some were victimized 60 or more times during the test period. For many small companies, being knocked off the Internet for a week means being knocked out of business for good.

The Computer Security Institute/FBI also documents the problem in a widely reported study on computer breaches. This year’s survey of 538 respondents found 85 percent experiencing computer intrusions, with 64 percent serious enough to cause financial losses. Estimated losses from those willing to provide the information tallied \$378 million, a 43 percent increase from the previous year.

A nationwide public opinion poll released last year by ITAA and EDS showed that an overwhelming majority of Americans, 67 percent, feel threatened by or are concerned about cyber crime. In addition, 62 percent believe that not enough is being done to protect Internet consumers against cyber crime. Roughly the same number, 61 percent, say they are less likely to do business on the Internet as a result of cyber crime, while 33 percent say crime has no effect on their e-commerce activities. The poll of 1,000 Americans also revealed that 65 percent believe online criminals have less of a chance of being caught than criminals in the real world, while only 17 percent believe cyber criminals have a greater chance of being caught.

These threats collectively represent a chipping away at the trust that is so critical to the Internet. Thankfully, technology is moving faster than public policy ever could to secure the technology that will be dominate our economic future.

The Industry Securing the Internet: Information Security

Information security, or cyber security, is the multifaceted discipline that counteracts cyber crime and works to secure the Internet. Information security--or InfoSec--deals with cyber crime prevention, detection and investigation. How do we achieve improved security for the Internet of today and minimize the security challenges of tomorrow's Internet?

Cyber Security is Built From Technology, Processes and People

Too many times, the assumption is made that improving cyber security and fighting cyber crime can be done with technology alone. That is wrong. Just as the best alarm system

will not protect a building if the alarm code falls into the wrong hands, a network will not be protected if the passwords are given out freely. Failures in the “process and people” part of the cyber crime solution may, in fact, be the majority of the problems we see. Processes and people tend to be the more problematic elements of the Internet security puzzle. The two are closely linked. From a strategic point of view, the challenge is to make cyber security a top priority issue. Moving from platitudes to practical action requires the sustained commitment of senior management.

The goal is to embed cyber security in the corporate culture. That is not always easy to do. CEO’s want their IT systems to be as fast as Ferrari but as safe as an armored truck. Whenever tradeoffs arise, the bias is towards speed, not safety and security. The challenge for the IT sector and its customers working together is to provide security at the speed of business.

Organizations must be willing to invest in the development of comprehensive security procedures and to educate all employees--continuously. We call this practicing sensible cyber hygiene, a term that my friend Vint Cerf frequently uses as he speaks about these challenges around the globe. The primary focus of improving processes and changing behaviors is inside the enterprise. However, the scope of the effort must also take into account the extended organization—supply chain partners, subcontractors, customers, and others that must interact on a routine basis.

With cyber hygiene practices in place, companies can more effectively use the technologies that are available. A very simple example is that a company may diligently employ the latest virus detection software. But, if individual users within the company do not regularly heed messages to update virus profiles covered by the software, it renders the company’s security less effective.

Industry Plan for Cyber Security

ITAA and its members have been working to execute a multi-faceted plan designed to improve U.S. cooperation on issues of information security. However, Mr. Chairman, we would all be remiss if we believed it was just the IT industry that must cooperate within its own industry--we must work cross industry, and industry with government. Protecting our infrastructure is a collective responsibility, not just the IT community’s role.

We are working on multiple fronts to improve the current mechanisms for combating threats and responding to attacks through our role as a Sector Coordinator for the Information and Communications sector, appointed by the U.S. Department of Commerce. Through ITAA’s InfoSec Committee, our member companies also are exploring joint research and development activities, international issues, and security workforce needs. Elements of the plan include Information Sharing, Awareness, Education, Training, Best Practices, Research and Development, and International Coordination.

INFORMATION SHARING: Sharing information about corporate information security practices is inherently difficult. Companies are understandably reluctant to share sensitive proprietary information about prevention practices, intrusions, and actual crimes with either government agencies or competitors. Information sharing is a risky proposition with less than clear benefits. No company wants information to surface that they have given in confidence that may jeopardize their market position, strategies, customer base, or capital investments. Nor would they risk voluntarily opening themselves up to bogus but costly and time-consuming litigation. Releasing information about security breaches or vulnerabilities in their systems presents just such risks. Negative publicity or exposure as a result of reports of information infrastructure violations could lead to threats to investor – or worse – consumer confidence in a company’s products. Companies also fear revealing trade secrets to competitors, and are understandably reluctant to share such proprietary information. They also fear sharing this information, particularly with government, may lead to increased regulation of the industry or of electronic commerce in general.

Public policy factors also act as barriers to industry information sharing. One of the obstacles is the Freedom of Information Act (FOIA). Companies worry that if information sharing with government really becomes a two-way street, FOIA requests for information they have provided to an agency could prove embarrassing or costly. FOIA requests place the private sector’s requirement for confidentiality at odds with the public sector’s desire for sunshine in government information. We are working with Congressman Tom Davis (R-VA), Senator Robert Bennett (R-UT), and other key players on legislation to meet this concern.

Anti-trust concerns are a second potential legal hurdle to information sharing. Fortunately, such risks appear small. The antitrust laws focus on sharing information concerning commercial activities. Information Sharing Advisory Centers (ISACs) should be in compliance with the antitrust laws because they are not intended to restrain trade by restricting output, increasing prices, or otherwise inhibiting competition, on which the antitrust laws generally focus. Rather, ISACs facilitate sharing of information relating to members' efforts to enhance and to protect the security of the cyber infrastructure, so the antitrust risk of such exchange is minimal. The Justice Department has also indicated that there are minimal antitrust concerns involving properly structured joint industry projects for dealing with externalities. An entity created to share information regarding common threats to critical infrastructure should fall into this category.

Given the changing nature of the cyber crime threat and in spite of the many business, operational and policy hurdles standing in the way, many companies in the private sector recognize the need to have formal and informal information sharing mechanisms. Internet Service Providers are an example of the latter circumstance. Because these firms provide networking capability commercially, these businesses often have extensive network security expertise. Such firms act as virtual Information Sharing and Analysis Centers, gathering information about detected threats and incursions, sanitizing it by removing customer specific data, and sharing it with customers.

The IT industry has adopted a formal approach to the information sharing challenge. In January 2001, nineteen of the nation's leading high tech companies announced the formation of a new Information Technology Information Sharing and Analysis Center (IT-ISAC) to cooperate on cyber security issues. The objective of the IT-ISAC is to enhance the availability, confidentiality, and integrity of networked information systems. The group has made excellent progress in the six months since its founding and is in the process of being formally "stood up," although information sharing is already beginning to take place within this ISAC.

The IT-ISAC is a not-for-profit corporation that will allow the information technology industry to report and exchange information concerning electronic incidents, threats, attacks, vulnerabilities, solutions and countermeasures, best security practices and other protective measures. Its internal processes will permit information to be shared anonymously. The organization is a voluntary, industry-led initiative with the goal of responding to broad-based security threats and reducing the impact of major incidents. Membership in the IT-ISAC is open to all U.S.-based information technology companies. It will offer a 24-by-7 network, notifying members of threats and vulnerabilities. The group also is clear on what it will not undertake. Excluded activities include standards setting, product rating, audits, certifications or dispute settlement. Similarly, the IT-ISAC is not a crime fighting organization. The nineteen Founding Member companies of the IT-ISAC, all represented at the announcement, are AT&T, Cisco Systems, Computer Associates, CSC, EDS, Entrust Technologies, Hewlett-Packard Company, IBM, Intel Corporation, KPMG Consulting, Microsoft Corporation, Nortel Networks, Oracle Corp., RSA Security, Securify Inc., Symantec Corporation, Titan Systems Corp., Veridian and VeriSign, Inc.

The group plans to evolve its information sharing activities over time, starting with IT companies and then moving across sectors. It is also expected that the ISAC will enable sensitive information to be shared between industry and government. But that sharing must be a two-way street, if it is going to be effective.

The Software Engineering Institute's CERT Coordination Center plays an information sharing role for numerous industries. The oldest and largest of information sharing programs, CERT is a Federally funded research and development center at Carnegie Mellon University in Pittsburgh. The organization gathers and disseminates information on incidents, product vulnerabilities, fixes, protections, improvements and system survivability. The organization strives to maintain a leak proof reputation while collecting thousands of incident reports yearly. These could be anything from a single site reporting a compromise attempt to a virus with worldwide impact.

The IT-ISAC is specifically designed to support the IT industry in this country. Other ISACs have been formed in the financial services and telecommunications industries. And I would like to mention two other groups that play an important information sharing role. [The Partnership for Critical Infrastructure Security](#) provides a venue for organizations from numerous industries to pool their knowledge and experience about information infrastructure risks and protections. PCIS also examines critical interdependencies among infrastructure providers and seeks common solutions to risk

mitigation. [The Partnership for Global Information Security](http://www.pgis.org) <<http://www.pgis.org>> provides a forum for executives from both the public and private sector in economies around the world to share information about InfoSec topics. PGIS members are focused on five areas for collaboration: sound practices, workforce, research and development, cyber crime and law enforcement and public policy. ITAA is proud to have played a leadership role in the formation of both organizations, and I sit on the Boards of Directors of both.

AWARENESS: ITAA and its member companies are raising awareness of the issue within the IT industry and through partnership relationships with other vertical industries, including finance, telecommunications, energy, transportation, and health services. We are developing regional events, conferences, seminars and surveys to educate all of these industries on the importance of addressing information security. An awareness raising campaign targeting the IT industry and vertical industries dependent on information such as the financial sector, insurance, electricity, transportation and telecommunications is being overlaid with a targeted community effort directed at CEOs, end users and independent auditors. The goal of the awareness campaign is to educate the audiences on the importance of protecting a company's infrastructure, and instructing on steps they can take to accomplish this. The message is that information security must become a top tier priority for businesses and individuals.

EDUCATION: In an effort to take a longer-range approach to the development of appropriate conduct on the Internet, the Department of Justice and the Information Technology Association of America have formed the [Cybercitizen Partnership](#). Numerous ITAA member companies and recently the Department of Defense have joined this effort. The Partnership is a public/private sector venture formed to create awareness in children of appropriate on-line conduct. This effort extends beyond the traditional concerns for children's safety on the Internet, a protective strategy, and focuses on developing an understanding of the ethical behavior and responsibilities that accompany use of this new and exciting medium. The Partnership is developing focused messages, curriculum guides and parental information materials aimed at instilling a knowledge and understanding of appropriate behavior on-line. The Partnership hosted a very successful event last fall at Marymount University in Northern Virginia that brought together key stakeholders in this area. Ultimately, a long range, ongoing effort to insure proper behavior is the best defense against the growing number of reported incidents of computer crime. The Cybercitizen website has received over 600,000 hits in the past year.

TRAINING: ITAA long has been an outspoken organization on the impact of the shortage of IT workers – whether in computer security or any of the other IT occupations. Our groundbreaking studies on the IT workforce shortage, including the latest, [“When Can You Start,”](#) have defined the debate and brought national attention to the need for new solutions to meet the current and projected shortages of IT workers. We believe it is important to assess the need for and train information security specialists, and believe it is equally important to train every worker about how to protect systems.

We have planned a security skills set study to determine what the critical skills are, and will then set out to compare those needs with courses taught at the university level in an effort to determine which programs are strong producers. We encourage the development of “university excellence centers” in this arena, and also advocate funding for scholarships to study information security. We commend the Administration and Congress for supporting training more information security specialists.

The challenge to find InfoSec workers is enormous, because they frequently require additional training and education beyond what is normally achieved by IT workers. Many of the positions involving InfoSec require US citizenship, particularly those within the federal government, so using immigrants or outsourcing the projects to other countries is not an option.

BEST PRACTICES: We are committed to promoting best practices for information security, and look to partners in many vertical sectors in order to leverage existing work in this area. In addition, our industry is committed to working with the government—whether at the federal, state or local levels. For example, we are working with the Federal Government’s CIO Council on efforts to share industry’s best information security practices with CIOs across departments and agencies. At the same time, industry is listening to best practices developed by the government. This exchange of information will help industry and government alike in creating solutions without reinventing the wheel.

While we strongly endorse best practices, we strongly discourage the setting of “standards.” Why?

Broadly, the IT industry sees standards as a snapshot of technology at a given moment, creating the risks that technology becomes frozen in place, or that participants coalesce around the “wrong” standards. Fighting cyber crime can be thought of as an escalating arms race, in which each time the “good guys” develop a technology solution to a particular threat, the “bad guys” develop a new means of attack. So to mandate a particular “solution” may be exactly the wrong way to go if a new threat will soon be appearing.

It is also critical that best practices are developed the way much of the Internet and surrounding technologies have progressed – through “de facto” standards being established without burdensome technical rules or regulations. While ITAA acknowledges the desire within the Federal government to achieve interoperability of products and systems through standard-setting efforts, the reality is that the IT industry can address this simply by responding to the marketplace demand. The marketplace has allowed the best technologies to rise to the top, and there is no reason to treat information security practices differently.

RESEARCH AND DEVELOPMENT: While the information technology industry is spending billions on research and development efforts—maintaining our nation’s role as the leader in information technology products and services—there are gaps in R&D. Frankly, for

industry, more money is frequently spent on “D”—development—then “R”—long-term research. Government, mainly in the Department of Defense, focuses its information security R&D spending on defense and national security issues. We believe that between industry’s market-driven R&D and government’s defense-oriented R&D projects, gaps may be emerging that no market forces or government mandates will address. Government funding in this gap—bringing together government, academia and industry—is necessary.

INTERNATIONAL: In our work with members of the information technology industry and other industries, including financial services, banking, energy, transportation, and others, one clear message constantly emerges: information security must be addressed as an international issue. American companies increasingly are global corporations, with partners, suppliers and customers located around the world. This global business environment has only been accentuated by the emergence of on-line commerce—business-to-business and business-to-consumer alike.

Addressing information security on a global level clearly raises questions. Many within the defense, national security and intelligence communities rightly raise concerns about what international actually means. Yet, we must address these questions with solutions and not simply ignore the international arena. To enable the dialogue that is needed in this area, ITAA and WITSA conducted the first Global Information Security Summit in Fall 2000. This event brought together industry, government and academia representatives from around the world to begin the process of addressing these international questions. A second Summit is planned for later this year to continue the dialogue. The governmental international linkages must be strengthened—and not just among the law enforcement and intelligence communities. Government ministries around the world involved in economic issues—such as our own Department of Commerce—need to be key players.

How Government Can Help

In many ways, solutions to cyber security challenges are no different than any other Internet-related policy issue. Industry leadership has been the hallmark of the ubiquitous success of our sector. Having said that, we also believe that government has several roles to play in helping achieve better cyber security and combating cyber crime:

- First and foremost, like a good physician practicing under the Hippocratic oath, do no harm. Excessive or overly broad legislation and subsequent regulation crafted in a rapidly changing technology environment is apt to miss the mark and likely to trigger a host of unintended consequences. In many instances, existing laws for crimes in the physical world are adequate to address crimes conducted in cyberspace. New legislation should always be vetted for circumstances that single out the Internet for discriminatory treatment.
- Practice what you preach. The rules of technology, process and people apply equally to the public sector. The U.S. government must lead by example in

preventing intrusions into agency websites, databanks and information systems. Leadership in this area means substantial investments of new money in information security technology and services. Responding to the issue by reallocating existing dollars from current programs is robbing Peter to pay Paul and likely to play out at the expense of the American public and their confidence in e-government. It also means insisting that government agencies implement rigorous information security processes and practice them on a daily basis. Making InfoSec part of the government culture will require extensive senior management commitment.

- Reach out to international counterparts for crucial discussions of cyber security, and in particular, how to most constructively and effectively enforce existing criminal laws in the increasingly international law enforcement environment fostered by the Internet and other information networks.
- Bring leadership to bear through existing structures including the new cyber security board that will likely be established by Executive Order later this year. ITAA, its members and the IT industry continue to work hard to develop collegial and constructive relationships with the leadership and staff of the Critical Information Assurance Office (CIAO), the Commerce Department (DOC), the National Institute of Standards and Technology (NIST), and the Critical Information Infrastructure Assurance Program Office (CIIAP) at NTIA, as well as the National Security Council (NSC), Department of Justice (DOJ), Department of Energy, the National Information Protection Center (NIPC), and the National Security Agency (NSA).
- Funding will also help in the areas of workforce development and research. We have a critical shortage of information technology professionals generally and information security specialists specifically. In general, we support legislation to increase the number of appropriately skilled workers in this critical area. We also support additional R& D funding.

Conclusion

Society's reliance on the Internet will only increase over time. The evolution of the Internet over these thirty-some years tells us that its possibilities are limited only by our imaginations. The prospect of ubiquitous commerce, brought about by wireless computing, could pose greater security challenges as we move forward.

Internet security is an enabler to continued progress, and without it, public trust could erode and the true limits of technology never be pushed. I submit to you that the market is moving quickly to establish and maintain public trust in this new and exciting medium.

In closing, I leave the committee with the following thoughts on securing the Internet.

- Internet security must continue to become the focus of corporate CEOs and Boards of Directors and their counterparts in the public sector. Internet security is economic security, and market forces will continue to draw the attention of the highest levels of corporate hierarchy. This is a beneficial development.
- The Internet will continue to evolve towards ubiquity. As it does, technological developments will move quickly to secure it, but implementing those technologies will be essential.
- Technology is only part of the answer. People and processes are the other key ingredients. Assuring that users and companies practice sound “cyber hygiene” is important to securing the Internet.
- Market forces are the key. These forces will prevent an erosion of trust, will contribute to efficiently developing security products, and will drive management at all levels to focus on Internet security.
- Educating young people about the need to be good cybercitizens—through programs such as the ITAA/Department of Justice/Department of Defense Cybercitizen Partnership--is one tool to fight cybercrime that needs wider support.

Thank you and I welcome any questions from the Committee.