Private Sector

BSA Cyber Security Survey 2002

BSA and IPSOS Public Affairs conducted a survey of IT professionals in June 2002. More than half of all IT professionals questioned (55%) felt that the risk of a major cyber attack on the US increased after September 11th and over a third of those questioned (38%) felt that the government was not adequately prepared to deal with such a threat. Most believed that government security responses to the threat of cyber attack should be even more vigorous than were preparations for Y2K though they don't believe this is occurring yet.

BSA US Business Cyber Security Survey 2002

BSA and IPSOS Public Affairs conducted a survey of IT professionals, US adults and US Internet users in July 2002. While a majority of IT professionals (58%) say that US businesses' ability to defend against a major cyber attack has improved since September 11th, nearly half (45%) say US businesses are still not prepared for a major cyber attack. In addition, 47% of IT professionals thought it was "likely" US businesses would be subject to a major cyber attack in the next year while only 25% of US adults had the same concern.

2001 CSI/FBI Computer Crime and Security Survey

An annual survey of computer security practitioners from US corporations and government agencies conducted by the Computer Security Institute and the Federal Bureau of Investigation's San Francisco Computer Intrusion Squad. Ninety-one percent of respondents detected computer security breaches in the twelve months preceding the survey and sixty-four percent acknowledged financial loss due to computer breaches. For the fourth year in a row more respondents (70%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack.

2001 Information Security magazine Industry Survey

Information Security magazine conducts an annual online survey the most recent of which took place from late July 2001 to early August 2001 and was completed by 2,545 information security professionals. The magazine reported the results in its October 2001 issue. Although corporate funding for information security increased overall, nearly one-third of companies froze security spending at sometime in 2001 due to adverse economic conditions. While the top priority of security professionals is securing the network perimeter from external attack, 'insider' security incidents occur far more frequently than 'external' incidents. This problem is further exacerbated in a layoff economy when poor security becomes an even greater risk.

The Cyber-Security Summit: Executive Summary

The Cyber-Security Summit was a conference hosted by Booz Allen Hamilton and Lucent Technologies/Bell Labs on 11 December 2001. It was held simultaneously in video-linked facilities in Washington, DC and Murray Hill, NJ. The participants included Fortune 1000 executives and senior government officials. The common themes discussed: adequate information network defenses are essential to business continuity and national security; technology can strengthen cyber-security when accompanied by appropriate organizational policies and practices; customers must demand greater security from software vendors and service providers; and information security solutions must cut across functional silos within organizations. Participants concluded that cyber-security requires organizations to breach the walls and misunderstandings that often divide the public and private sectors.

Ernst & Young Information Security Survey 2001

Between October and November 2000 the UK office of Ernst & Young International conducted face to face and telephone interviews using a structured questionnaire among a representative sample of CIOs, IT Directors and business executives in countries across Europe. Over half of the organizations surveyed were found not to have an e-commerce strategy while most were pursuing e-commerce activities including maintaining a website for one-way information (73%), maintaining an intranet for one-way information (60%), and conducting electronic transactions (34%). The nature of initiatives currently being pursued (largely one-way information) indicates that many businesses are taking a relatively cautious approach to e-commerce and security continues to be the biggest concern. Only thirty-three percent of respondents expressed confidence in their organization's ability to detect a security breach.

Ernst & Young Fraud: The Unmanaged Risk

An international survey of the effect of fraud on business produced by the UK firm of Ernst & Young and released in May 2000. Questionnaires were sent in October 1999 to senior executives in 10,000 major organizations in 15 countries of which 739 responses were collected from Australia, Canada, France, India, Italy, New Zealand, South Africa, UK, US, Ireland, Germany, Switzerland, Sweden, Monaco, and Luxembourg. The survey asked questions about all types of fraud, however, computer-related fraud was found to be more likely to be viewed as a threat than any of the other types of fraud in the questionnaire with sixty percent of respondents fearing that such a fraud is likely or very likely. The survey also found that eighty-five percent of respondents are moderately or completely confident that their controls can prevent such fraud.

KPMG E-Commerce and Cyber Crime: New Strategies for Managing the Risks of Exploitation

In 2000, a white paper was prepared by KPMG LLP the US member firm of KPMG International. The report found that many organizations in the US have not adapted their security strategies to the interconnectedness of the electronic world and consequently tend to think of security and risk management solutions in a disjointed fashion. A holistic strategy for cyber defense and preparedness can prevent liability on behalf of client management, avert potential lawsuits or regulatory action, recover lost revenue, and maintain or restore the reputation and integrity of the firm. Integrated security policies, employee training, and awareness can be a competitive advantage in a business environment increasingly dependent on security and reliability of computer networks.

KPMG 2001 Global E-Fraud Survey

In 2000, KPMG Forensic and Litigation Services practices worldwide sent questionnaires on e-commerce and e-fraud to more than 14,000 senior executives of the largest public and private companies in twelve countries: Australia, Belgium, Canada, Denmark, Germany, Hong Kong, India, Italy, South Africa, Switzerland, UK, and the US. 1,253 respondents completed questionnaires and sixty-two percent said they had embraced e-commerce in their businesses. However, only nine percent of respondents indicated a security breach within the past twelve months. The report finds, based on recent media accounts, that this estimate is low and suggests a variety of explanations including reluctance to report such information (only 62% of respondents elected to answer this question), respondents not having been made aware of security breaches that occurred within their organization, and attacks going undetected. In another startling revelation, respondents indicated overwhelmingly that security of credit card numbers and personal information were of paramount importance to consumers, however, less than thirty-five percent reported having security audits performed on their systems.

The report also finds that the 'onion' model of security is currently considered by many experts to be the most effective and safest approach to managing risks associated with e-commerce. The 'onion' model consists of various layers of properly implemented protection mechanisms: encryption, firewalls, intrusion detection systems, incident response procedures, monitoring and audits performed by external specialists.

Pricewaterhouse Coopers European Economic Crime Survey 2001

The survey interviewed senior representatives of more than 3,400 companies, non-profit organizations, and government bodies in fifteen Western and Central European countries. Forty-two percent of the larger European firms fell victim to fraud during the last two years, the average cost of which was €6.7 million across all firms. Asked to identify types of fraud they believe to be most prevalent, cyber-crime polled a lowly six percent, but forty-three percent of respondents identify it as a key concern for the future. In fact the authors of the report found cyber-crime was actually experienced by thirteen percent of firms who had suffered a fraud and is already a threat and not just an "issue for the

future." The report also found that many organizations do not act on lessons learned – less than half implemented changes to improve their risk management procedures, leaving them open to fraud again. Public awareness and acknowledgement of the problem are prerequisites to tackling it effectively.

Public Sector

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (Gilmore Commission) Third Annual Report

The Advisory Panel began its work in 1999 to assess the level of terrorist threat to the US and completed this Third Annual report in December 2001. September 11, 2001 highlighted the urgency of their cause and this report has received arguably the most attention since the Panel's inception. Among the issues concentrated on are: State and Local Response, Health and Medical Capabilities, Immigration and Border Control, Security Against Cyber Attacks, and Roles and Missions on the Use of the Military. It is significant that cyber security and cyber threats have been a part of the Panel's work since 1999, the level of threat they represent was recognized even then. The report also recommends that Congress create an independent commission to evaluate programs designed to promote cyber security, to identify areas where requirements are not being met, and to recommend strategies for improving cyber security.

Congressional Research Service Report for Congress: Cyberwarfare

The report, published in June 2001, notes that there is ample evidence that terrorist organizations use cyberspace to conduct the business of terrorism but insufficient evidence that the Internet itself could be used as a tool of violence to achieve political objectives. Because of the high stakes involved, a comprehensive strategy is recommended to mitigate the damage a first attack could cause.

Commission on Child Online Protection: Report to Congress, 20 October 2000

In October 1998 Congress enacted the Child Online Protection Act and established the Commission on Child Online Protection to study methods to help reduce access by minors to certain sexually explicit material defined in the statue as harmful to minors. The Commission concluded that no single technology or method will effectively protect children from harmful material online. The Commission determined that a combination of public education, consumer empowerment technologies and methods, increased enforcement of existing laws and industry action are needed to address this concern.

General Accounting Office, Information Sharing: Practices That Can Benefit Critical Infrastructures

In this October 2001 report to Congress the General Accounting Office sought to identify ways the federal government could mitigate risks to the nation's critical computer-dependent infrastructures, many of which are privately owned. All of the organizations

interviewed identified trust as the essential underlying element to successful relationships among federal agencies and public and private sector entities. Other critical success factors included establishing effective and appropriately secure communication mechanisms such as regular meetings and secure websites; obtaining support of senior management regarding sharing of potentially sensitive information and commitment of resources; and ensuring organization leadership continuity. Congress has a role to play in monitoring the progress in meeting key critical infrastructure protection goals, including improved information sharing, and by clarifying the way federal agencies may use sensitive information provided for critical infrastructure purposes.

Information System Security: Army Website Administration, Policies, and Practices

This report is part of a series undertaken by the Department of Defense (DoD) that will cover all branches of the armed services and the DoD at its conclusion. The results of this report for the Army were disappointing. The report found that inappropriate and sensitive material was available on the Army's publicly accessible websites in contravention of Army Website Policy and recommended revised risk management assessment and training.

Internet Policy Institute's Briefing the President

The Internet Policy Institute sponsored the publication of a series of essays on policy issues related to the Internet during the 2000 presidential election campaign. The thirteen essays, released monthly from November 1999 to November 2000, were collectively entitled *Briefing the President: What the Next President of the United States Needs to Know About the Internet and its Transformative Impact on Society* and intended to be presented to the new president-elect after the election. Below a selection of essays has been abstracted here.

The Internet, Law Enforcement and Security by Scott Charney, PricewaterhouseCoopers

The Internet is a technology that is far more powerful than most that are placed in the public domain, so powerful in fact that it is no longer true that only States have access to weapons of war. The government, reluctant to regulate the Internet and risk stifling innovation, has repeatedly stated that the private sector is primarily responsible for protecting the nation's critical infrastructures. In so doing, the government has in large part ceded public safety and national security to markets while these private sector entities' primary mission is not to protect public safety and national security but to protect and increase profitability. The issue of critical infrastructure protection requires societal debate and consensus, and markets should not be allowed to dictate the choices.

Shaping the Internet Age by Bill Gates, Microsoft Corp.

The Internet is making the world smaller through improved communication and simplifying logistical barriers for businesses. It breaks down barriers between (and within) nations, opening up economies and democratizing societies. The Internet makes it possible to distribute any kind of digital information, from software to books, music, and video, instantly and at virtually no cost. Protecting intellectual property and regulating global commerce are significant challenges, however, and we are only at the dawn of the Internet Age.

The Economy and the Internet: What Lies Ahead? by Robert Litan and Alice Rivlin

Expanding the use of the Internet creates a significant potential for increasing national productivity and raising the standard of living over time. The results of increased competition, nationally and internationally, should be lower profit margins, more efficient production, and greater consumer satisfaction. The greatest impact of the Internet may not be felt in e-commerce per se, but in lower transactions costs involving information flows (ordering, invoicing, etc.) across existing sectors of the economy and improved management efficiencies in product development, supply chain management, and a variety of other aspects of business performance.

The Internet and the New Economy by Alan Blinder

Blinder writes that some evidence points to an increase in productivity growth occurring at roughly the same time Internet technologies were diffusing throughout the economy, but there is not enough historical perspective at present to determine whether we are in a New Economy or not. Retailing over the Internet may offer many benefits to consumers, but such gains do not affect productivity growth. The greatest productivity benefits of the Internet may be in business-to-business commerce where many firms claim that putting their supply chains online has led, or will lead, to major cost savings.

The Internet and the Future of Democratic Governance by Sen. Patrick Leahy, D-Vt and Rep. Robert Goodlatte, R-Va

One of the great contributions to democratic governance that the Internet promises in the US is that citizens from all around the country can have access to government documents physically stored in Washington, DC. Increased openness would increase the accountability and responsiveness of the federal government. The same principle would also apply to the state and local levels. Internationally, the Internet has made vast amounts of information from around the world accessible to people with no access to a free press, and is proving a vital tool for expressing dissent under totalitarian regimes as in Serbia recently. The free flow of information and ideas is what makes the medium so dynamic and an effective democratic tool. US Internet policies must, therefore, respect the First Amendment and any step the government may take to ensure the Internet is safe

for kids and free from criminal activity must balance these goals with strong protections for free speech and expression.

The Internet, Consumers and Privacy by Ellen Alderman and Caroline Kennedy

A recent survey by the Federal Trade Commission found that 92% of Americans are concerned (67% very concerned) about the misuse of their personal information on the Internet. The same report also indicated that this apprehension accounted for lost online sales with estimates varying from $2.8 billion in 1999 to as much as $18 billion in 2002 (compared to a projected total of $40 billion in online sales). Protecting privacy on the Internet is becoming a necessary condition for e-commerce. Public concern about privacy online has reached a critical point and other nations have already passed comprehensive privacy legislation.

The Internet and Education by Robert O. McClintock, Columbia University

The Internet broadens educational opportunity, but also will increase educational expenditures. Effective use of technology in education requires substantial and continuous spending; one-time initiatives will set states up for long-term failure. To make full use of the Internet, schools need to develop annual capital budgets for continuously upgraded production tools and expanded training support.

The Internet and Citizens: Advanced Technology in All Communities by Robert E. Knowling, Jr., Covad Communications

Knowling writes that there is a very real risk that those communities which could benefit most from the Internet -- rural, low income and minority Americans -- will miss out on these opportunities because of lack of access to new technologies. This "Digital Divide," as it is called, undermines the entire country's ability to maintain its competitive edge in the world economy.

Closing the Digital Divide: An Initial Review by Ernest J. Wilson III, University of Maryland and Center for Strategic and International Studies

This essay examines the digital divide from a global perspective. The Internet is widely diffused in North America, but 98% of Latin Americans, 99.5% of Africans, and about 98% of Asians are not connected to the Internet. Moreover, while telephone penetration is growing, half the world's people still have never heard a dial tone. The gap between OECD countries and less developed countries (LCDs) continues to grow, both in terms of information and communication technologies and incomes, but like in developed countries, a causal link has failed to be established between the introduction of these technologies and economic growth. There is still not enough historical data for conclusions to be drawn.