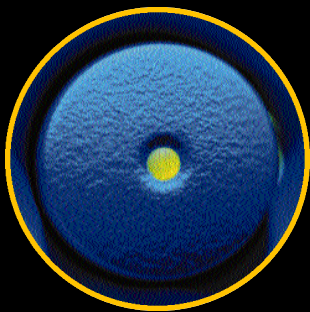


SIIA's Report on Global Software Piracy 2000

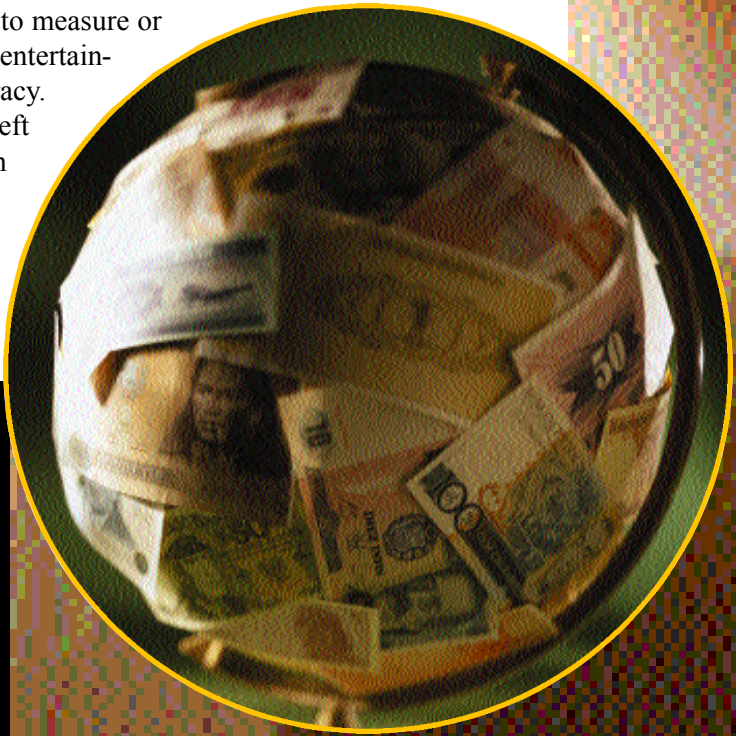
SIIA's Report on Global Software Piracy 2000



Introduction

The Software & Information Industry Association (SIIA) is pleased to present its sixth annual "Report on Global Software Piracy". This report examines business application software piracy in 1999, using data collected from a variety of sources and analyzed using strict research methodology. It is SIIA's hope that the conclusions reached in this report will serve as a wake-up call to governments, businesses and individuals throughout the world that software piracy adversely affects a nation's economic well-being, stifles individual creativity and discourages businesses' investments. Put simply, piracy of such magnitude must be stopped. The SIIA report estimates the revenue lost by software publishers and analyzes software piracy data for 80 nations, from Austria to Uruguay and most points in-between. This report does not include revenues lost to governments through income tax, sales taxes or value-added taxes. Nor does it account for job losses in the core software and packaged business software industries and in the retail sector. These losses should not be discounted merely because they are not contained within the pages of this report. These components of a nation's economy represent additional significant benefits that could be applied to economic growth, had they not been lost through unauthorized copying of computer software.

The SIIA report also does not attempt to measure or estimate revenue losses from educational, entertainment and electronic (Internet) software piracy. Nor does this report cover losses due to theft of digital information. This does not mean that revenue losses from piracy in these areas are not significant. In fact, SIIA believes revenue losses from these areas are considerable, and they should not be disregarded.





The Bottom Line

In 1999, business PC application software accounted for worldwide revenues of \$21.6 billion – a 19% increase over last year. SIIA calculated 1999 global revenue losses due to piracy in the business application software market as \$12 billion. Most of this increase is due to an increased use of software – pirated units increased 34% over 1998, and more use means higher losses.

A smaller pirated *share* of a much larger market leads to an increase in revenue lost since a larger number of units are pirated.

Revenues Lost to Software Piracy by Region

(thousand U.S. dollars)

	1997	1998	1999
Western Europe	\$2,519	\$2,760	\$3,630
Central Europe	561	640	409
North America	3,074	3,196	3,631
Latin America	978	1,045	1,128
Asia/Pacific	3,916	2,955	2,792
Middle East	206	190	284
Africa	186	190	194
WORLD TOTAL	\$11,440	\$10,976	\$12,163

The Importance of Strong Intellectual Property Protection for Software

Strong intellectual property protection for software is an important part of any nation's economic growth and development. Empirical and anecdotal evidence clearly show the enormous economic and social benefits of a legitimate, thriving software industry wherever software is effectively protected by a nation's laws and law enforcement agencies. Although the United States maintains its strong leadership position in publishing and distributing software and digital content, other nations are also reaping the rewards of actively encouraging and supporting a strong local software industry. These rewards are most visible in the nation's improved employment and national wealth. Despite obvious economic and social benefits, the development, distribution and marketing of domestically produced software remains confined to a small group of nations. This is due in large part to the failure of many nations to encourage their residents, entrepreneurs and businesses to develop, distribute and market software through enactment and enforcement of strong intellectual property protections for computer software.

Strong intellectual property protection has numerous benefits. It:

- Encourages individuals and businesses to create innovative software applications and improve upon existing applications.
- Encourages an indigenous software industry that can tailor products to local conditions.
- Ensures new ideas and technologies are widely distributed.
- Promotes value and investment in the national economy.
- Encourages technology transfers between nations.

Strong copyright protection is extremely important for computer software in less-industrialized countries. The software industry is one area where local businesses can compete effectively with multinationals in both local and foreign markets. Massive capital investment is not necessary nor is acquisition of expensive foreign technology. In fact, local entrepreneurs often know the local needs and markets better than the multinationals and can exploit that knowledge. However, without adequate copyright and other protection, those local companies that create valuable software will soon find that others will copy their programs without permission and without remuneration, thereby decreasing their incentives to create and market new programs.

The Essential Elements Of An Effective Intellectual Property System

An effective intellectual property system is one that adequately protects its nation's software creations and inventions.

First and foremost, each nation must enact appropriate laws. "Appropriate," in this context, means the laws should acknowledge the rights of creators and owners of computer software, be comprehensive and leave no doubt as to what rights and remedies are granted in the law. Copyright protection should comply with international standards for the protection of software as set forth in the Berne Convention for the Protection of Literary and Artistic Works, the World Trade Organization (WTO) Agreement on Trade-Related Aspects of Intellectual Property (TRIPs) and the World Intellectual Property Organization (WIPO) Copyright Treaty.

Second, the courts and the appropriate government law enforcement agencies should effectively enforce the laws. To ensure meaningful protection of intellectual property rights in software creations, it is

essential that the nation's courts enforce the laws and that they do so rapidly and without undue procedural entanglements. In appropriate cases, the government bodies responsible for enforcement activity, such as the federal and local police, should conduct raids and seize and destroy the equipment and devices used by software pirates to engage in their illegal activities. The nation's customs agency should also take steps to protect pirate software from entering or leaving the country and, when appropriate, should seize pirate and gray market software at the border.

Finally, the public should be educated and understand the protections afforded to computer programs under copyright and other intellectual property laws. As technology advances and computer and communications technologies converge, any individual sitting at a PC has the opportunity to become a publisher and distributor. It is essential that the public be made aware of the importance of intellectual property protection for software and digital content and have some understanding of the laws that protect them. Once educated, these individuals will be more likely to respect the rights of software producers and not intentionally or unintentionally infringe these rights.

Legal Protection Provided to Software

Copyright law, in the United States and in most other countries, provides legal protection for software from the moment the software is created. Copyright law generally protects software and other forms of intellectual property by giving the owner of the software exclusive rights to control its

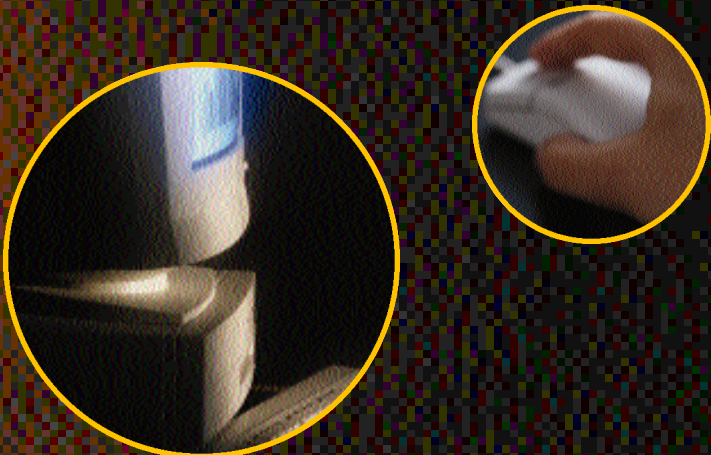


use by others. In the United States, with some exceptions, it is a federal offense to duplicate and distribute software without the copyright owner's permission. Although most software creators rely on copyright law to protect their software, other types of intellectual property protection – such as the protections afforded by patent law and state trade secret law – provide additional protection for software.

Federal legislation in the United States now makes it a crime to traffic in counterfeit goods (18 U.S.C. § 2320), reproduce or distribute copyrighted works (18 U.S.C. § 1831 et. seq.) or sell trade secrets (18 U.S.C. § 1030). In response to the software piracy problem that exists in the United States, U.S. government law enforcement agencies have organized units specially trained to investigate and prosecute software piracy. The U.S. Department of Justice, for example, formed the

The Essential Elements To An Effective Intellectual Property System

1. Enact appropriate laws.
2. Effectively enforce the laws.
3. Educate the public.



Computer Crime and Intellectual Property Section, and the FBI has computer crime squads in a number of major cities. The U.S. Customs Service and U.S. Postal Inspectors also continue to actively pursue these types of cases both domestically and internationally.

Internationally, the standards for copyright protection of software are set forth in the Berne Convention for the Protection of Literary and Artistic Works and the WIPO Copyright Treaty, which are both administered by the WIPO, and the TRIPs Agreement, which falls under the auspices of the WTO. These international agreements provide generally that copyrightable computer programs (including application programs and operating systems), whether in source code or object code, must be protected on a nondiscriminatory basis in each country that is party to the agreement. These agreements further set forth minimum standards defining and safeguarding the economic interests of creators of computer programs.



United States Enacts New Legislation to Aid the War Against Piracy

On December 9th, the president signed a law that increased some of the penalties for copyright infringement by 50 percent. The Digital Theft Deterrence and Copyright Damages Improvement Act of 1999, Public Law No.


106-160, amends section 504(c) of the Copyright Act, resulting in the first increase in copyright damages since 1988. Under Section 504(c) of the Copyright Act, a copyright owner may choose to recover statutory damages for infringement in place of actual damages and lost profits. Prior to enactment of the act, the amount of statutory damages that could be awarded by a court ranged from \$500 to \$20,000 per copyrighted work infringed. When the infringer is able to establish that its infringement was unintended for personal gain, however, the court may award statutory damages as low as \$200 per work infringed. Conversely, when willful infringement is proven, statutory damages may be awarded up to \$100,000 per work infringed.



The act increases the available statutory damages award for copyright infringement from the previous range of \$500 to \$20,000 to a range of \$750 to \$30,000. In cases of willful infringement, the cap was raised from \$100,000 to \$150,000. Given that the levels of statutory damages had not been changed for over 10 years and there have been numerous significant changes in the economy, business practices and technology during that 10-year period, the time was certainly right to increase statutory damage levels. The increase ensures that the sanctions provided under U.S. copyright law continue to be sufficient to remove any financial gain from the infringement and to deter future infringements. In addition, increasing statutory damages should aid the U.S. government in its attempts to convince countries throughout the world to improve the sanctions for copyright infringement provided for under their copyright laws. The act also requires the U.S. Sentencing Commission to “promulgate emergency guideline amendments” to implement the No Electronic Theft (NET) Act.¹ This provision responds to complaints by SIIA and other organiza-



¹ The NETAct criminalizes the willful infringement of copyrighted works, including by electronic means, when the infringing party derives no direct financial benefit from the infringement but infringes a party's copyright by reproducing or distributing one or more copyrighted works (during any 180-day period) having a “total retail value of more than \$1,000.” Penalties include imprisonment up to six years, and fines, depending upon the seriousness of the infringement and the damage to the copyright holder. The NETAct directs the U. S. Sentencing Commission to implement sentencing guidelines “sufficiently stringent to deter such a crime,” and “provide for consideration of the retail value and quantity of the items” See 28 U.S.C.A. § 994 NOTE.



tions that there have been virtually no prosecutions under the NET Act, in part because of the absence of appropriate sentencing guidelines. On April 6, 2000, the Sentencing Commission enacted amendments to the guidelines as required by the act.

Software piracy is defined as the unauthorized copying of computer software, which constitutes copyright infringement, for either commercial or personal use. Although there are many reasons why people pirate software, usual reasons include greed, carelessness, ignorance of the law or general disregard for software as valuable intellectual property. People who duplicate software to trim costs may do so under the erroneous belief that “everyone else is doing it.” Others may mistakenly believe it is legal to make and distribute copies so long as the copier derives no profit from the distribution or use. Still others may truly believe that software copying is a harmless activity that “doesn’t hurt anyone” or “isn’t really stealing.”

During the past two decades, systematic software piracy has become an increasing concern to businesses and software developers throughout the world. Recently, the problem has grown much worse. The proliferation of computers, internal computer networks and the Internet has made the illegal reproduction and distribution of protected material much easier to accomplish and more difficult to police.

Increased use of electronic software distribution may eventually reduce software theft, because technologies can be built in to prohibit further distribution. New business

models including the application service provider model (ASP) may also help reduce piracy through software hosting on the service provider’s server as opposed to the user’s desktop. The ASP model is still relatively new, so its potential for reducing piracy cannot yet be estimated.

The advent of more affordable CD-ROM recorders (CD-R’s) has led to their proliferation into personal computers. The increased ease of making unauthorized material can only mean an increase in piracy of intellectual property.

Unfortunately, many nations and their domestic businesses view software piracy as an easy way to bring themselves into the information-based global economy. All too often, we have found governments making half-hearted attempts to control or eliminate software piracy while turning a blind eye to the rampant illegal copying and selling of software in their own backyards. As this report shows, such myopia is not confined to underdeveloped nations or those with low national incomes. Key offending nations include Singapore, France, Italy, Greece, Argentina, Brazil and Israel.

Types of Software Piracy

Software piracy can be committed in a wide variety of ways, including:

- **Softlifting:** purchasing a single licensed copy of software and loading the same copy onto several computers, contrary to the license terms. For example, the sharing of software with friends, co-workers and others.
- **Internet:** making unauthorized copies of copyrighted software available to others electronically.
- **Software counterfeiting:** the illegal duplication and distribution of copyrighted software in a form designed to make it appear to be legitimate.
- **OEM unbundling:** selling stand-alone software that was intended to be bundled with specific accompanying hardware.
- **Hard disk loading:** installing unauthorized copies of software onto the hard disks of personal computers, often as an incentive for the end user to buy the hardware from that particular hardware dealer.
- **Renting:** unauthorized rental of software for temporary use, like you would a video.

The numerous ways in which software piracy occurs, the ease of duplication and the high quality of pirated software present a significant problem to the software industry. Unlike analog products subject to illegal copying, such as audiotapes and videotapes, there is no degradation in the quality of software from copy to copy. A program that reflects unprecendented technology, years of effort and millions of development dollars can be duplicated or illegally distributed in minutes with the touch of a button. Any PC user can duplicate a product priced from \$20 to \$20,000 for no more than the cost of a blank CD or at no cost, and that user can make one, a dozen or a thousand functional copies.

The unauthorized copying of personal computer software for use in the office or at home or “sharing” of software among friends and co-workers is the most pervasive form of piracy encountered and is estimated to be responsible for more than half the total revenues lost by the industry.

In The Trenches

The following examples illustrate the various scenarios under which piracy occurs. These real-life stories depict how software piracy affects the industry as a whole.

Piracy In The Workplace

This report calculates losses due to piracy for business application software at \$12 billion in 1999. This loss is solely attributed to businesses and organizations using business application software illegally. Here is one common scenario.

ATY Company believed that it complied with the copyright law. It set up a policy detailing how software should be acquired and what could happen to employees found to have unauthorized software on their computers. However, ATY did not properly implement this policy by conducting periodic software audits to ensure that installed software was properly licensed. When an employee of ATY Company called the software company for product support, the company discovered that ATY had not licensed its software. Even though ATY believed it had taken every necessary action, it failed to take the essential step of auditing its computers and networks to ensure that the policy was being followed. After the software company notified ATY of its violation and threatened a lawsuit, ATY agreed to pay a fine for the unauthorized software. In addition to the six-figure settlement, ATY was required to destroy all illegal software installed on its computers and to license the software so that its employees who needed the software had an authorized copy. Had ATY audited its computers, it would not have had to pay such a fine.

Counterfeiting: The Far East and Your Own Backyard

Not far from the bustling tourist areas in Singapore, a shopping center called Sim Lim Square hosts dozens of shops selling hundreds of CD-ROM titles for as little as \$5 each. At a quick glance, these shops appear to be selling legitimate CDs. On closer inspection, however, the CDs are actually counterfeits.

Counterfeits can be identified by close inspection of the discs, documentation (if any) and packaging. Poorly reproduced color, misplaced trademark logos, missing documentation, and typographical errors are

Piracy & the Internet

Technology and the Internet have come a long way since the Internet's inception, creating various avenues of how one transfers data over the Internet, such as: Web sites, e-mail, online chat, file transfer protocols (FTP), and the list goes on and on. Though this may be good for evolving the Internet into a global information center, it is not so good for preventing software piracy from occurring. In fact, these avenues create ways for piracy to flourish. Now software pirates can use these avenues as ways to communicate and share files with one another in real time.

Today people use Internet Relay Chat (IRC) to discuss just about any subject with anybody, anywhere, in real-time. People from all over the world gather in chat rooms where everyone within the chat room talks about certain subjects. Software pirates use IRC to create chat rooms in which they can come together and discuss software piracy. They converse about which crackz, warez, serialz, gamez and appz are the best; and then they tell where to find them for free or for an extremely discounted price. The chat rooms allow pirates to share with one another their warez and FTP sites that contain pirated software.

As the blatancy of piracy grows within such chat rooms and warez sites, the policing of such piracy grows as well, pushing pirates to pursue other ways to communicate and distribute pirated software with one another. Pirates are now using software and other technologies, such as Gnutella, to help them distribute unauthorized material to one another. Gnutella allows users to communicate in real time and distribute files amongst each other while being virtually anonymous. Gnutella may not necessarily have been developed for the software pirate, but has now become a software pirate's dreamed tool: pirating with virtual anonymity.

Pirates not only distribute software among themselves; they now are starting to reach out to the general public through online auction sites. Several auction sites have become virtual "pirate havens." Software pirates sell illegal copies of programs for a fraction of the original price through online auction sites. Pirates distributing illegal software attempt to deceive buyers into believing the listed item is legal by vaguely describing the software they are selling. SIIA has found that the majority of software auctions are not legitimate. SIIA has addressed the issue of piracy on Internet auction sites by conducting case studies and then releasing the results. SIIA has met with representatives of online auction sites to discuss the piracy problem and explore common-sense ways to eliminate piratical activity.

Through workings with both federal and state law officials, SIIA is taking great strides in conquering the battle against Internet piracy. Currently, SIIA works with the FBI on Internet piracy cases, and several of these cases have parlayed into having the pirate arrested. Through SIIA's concerted efforts, the future days of the Internet pirate are darkening.

Warez – term used to describe pirated software.

Appz – term for pirated software applications.

Gamez – the hacker term for pirated computer games.

Crackz – the term for breaking a software program's code(s). A crack can be used to make a software program's demo version into a full version.

Serialz – the term for serial numbers of software programs.

FTP – File Transfer Protocol, allows one to upload files and download files to a site. Software pirates who transfer warez to one another commonly use FTP sites.

IRC – Internet Relay Chat, allows multiple users to chat with each other on the Internet.

A Pirate's Tale

David's warez site, like so many other warez sites, contained a number of illegal software programs for download. All one had to do to download these illegal software programs was click on the various advertisements on David's site. Each time someone clicked on an advertisement, the advertiser added a dime to David's bank account. Once the same person had clicked on a certain number of advertisements, David then had a window pop up with the password to his protected section allowing access to the illegal software.

David had hundreds of software programs in his download section. In fact, he had so many his ISP increased his service charge for using so much bandwidth. SIIA was notified of this warez site from one of its members and ordered him to cease and desist his illegal activity. After years of reaping in the money from advertisers off his warez site, David was forced to permanently close his warez site on July 3, 1999.

But David enjoyed the easy money he received from his warez site too much to give up that easily, so now instead of operating his warez site, David mailed illegal software on "burned" CDs to his clients. David advertised his software piracy business in various newsgroups, online auctions, and chat rooms. It was this way that he met this new client, Jimmy.

His latest client went strictly by the name of Jimmy, and that was fine by David as long as Jimmy paid on time and in cash. Jimmy had initially contacted David by e-mail; he must have got the e-mail through one of the chat rooms that David frequents. David knew Jimmy was going to be a future client because the very first question Jimmy asked David was what happened to his warez site.

Jimmy wanted copies of graphics software and a couple of the latest business applications. Jimmy said that he needed these to start his own graphic design studio. David didn't care what business Jimmy started as long as he paid, and that Jimmy did. First it was \$75 for a graphics application, then it was \$300 for a compilation of graphics and business programs. David was profiting from Jimmy now, for it cost David only a few dollars to make copies of the software. Jimmy paid David a total of \$750 for the software. The suggested retail price of the software received by Jimmy was approximately \$10,000.

In October 1999, David was just about finished with Jimmy's order down in his basement. He had made his last duplicate of the latest, most expensive graphics application, and now all he had to do was pack and ship the pirated CDs to Jimmy. But then the knocks came...

If only David hadn't answered the door that Saturday, things would be different. Things would be a lot better than they are right now. David answered the knocks.

"Hello, may I help you?" David asked as he opened up his front door. But it was too late.

"Hi, I'm Jimmy." The FBI agent replied with a smile, and with that quick introduction, the FBI proceeded to arrest David for copyright infringement. By the end of the day, the FBI had found thousands of records showing distribution of unauthorized software. The seized records would be used as evidence in the case against David. In addition, they also seized David's computer hardware and software.

Everyday in jail, David contemplates the "what ifs."

"What if I wouldn't have answered the door?" "What if I never responded to Jimmy's e-mail?..." And the list of "what ifs" goes on and on. However, the one "what if" that haunts David the most is...

"What if I never committed piracy?"

When it was all said and done, David's records showed that he had sold over \$3 million worth of software to clients from 15 different countries. David's inventory of software included everything from computer games to graphic software to business tools to even some engineering applications. David now is looking at paying \$250,000 for his piracy acts once he finishes his five years in prison.

This story is based on a true event.

warnings the software may be counterfeit. For software publishers, the cost of counterfeiting is measured in lost sales and customer disappointment. End users who buy counterfeits quickly find that they suffer from a lack of technical support and documentation and the very real risk that the counterfeit software contains viruses and incompatible or nonfunctioning software.

Although we would like to be able to say that counterfeit software is limited to the Far East, this is unfortunately not the case. In the United States, for example, SIIA has obtained preliminary injunctions against numerous distributors who sold software at organized trade shows. The FBI and local law enforcement officials have also pursued individuals selling unauthorized software.

On October 27, 1999, 48-year-old David Pugh was arrested after a five-month investigation by the Florida Department of Law Enforcement. A search of Pugh's home revealed more than 1,000 pirated software applications. Investigators determined that Pugh's sole source of income during the past 12 years was derived from the sale of pirated software. Pugh was sentenced to 30 months in a Florida penitentiary following his conviction for dealing in stolen property and grand theft. Another such action by the Florida FBI resulted in a one-year prison term with restitution of nearly \$200,000.

Internet Piracy for Profit and Reputation

Jeffrey Levy, a 22-year-old senior at the University of Oregon, was sentenced to two years probation for illegally distributing copyrighted software and other material via his Internet site. Although Levy was the first person to be convicted under the 1997 NET Act, his sentence was light. Under the NET Act, Levy could have received up to three years in prison and a maximum fine of \$250,000.

The fact that some software pirates are not making a profit from the software they distribute does not change the illegal nature of the activity. Because the piracy took place over the Internet rather than in a non network environment also does not change the illegality of the distribution.

Copyright and other intellectual property laws apply in cyberspace as they do in the real world.

Internet service providers (ISPs) or Internet access providers (IAPs) may be liable for copyright infringement if their users illegally copy or distribute software through downloading, uploading or transmitting software files without the copyright owners' authorization and if they fail to take advantage of the "safe harbor" provisions of the Digital Millennium Copyright Act (17 U.S.C. 1201).



Unauthorized Rental: A Deal Too Good To Be True

In North Carolina, a storefront retailer named Software Exchange allowed customers to take software home for a fraction of the retail price, calling it a "nonrefundable deposit," as long as the customer returned the software in several days. Because Software Exchange did not have authorization to distribute software in this fashion, a civil lawsuit was filed by copyright holders. The Copyright Act makes it absolutely clear that the rental of software is illegal, unless it is expressly authorized by the copyright owner.

Unauthorized software rental operations promote software piracy by giving end users a convenient and inexpensive way to reproduce computer programs illegally. Because the risk of unauthorized end user copying is so great, rental operations should only be permitted when expressly authorized by the software producer and the software producer is able to control the terms and conditions of such rental.

The Ever-Changing Face of Piracy

The face of software piracy is ever-changing, especially in the online world. With recordable CD ROM drives (CD-R's and CD-RWs) being built into an increasing number of computers, the industry is faced with the growing threat of "home-pirates." These pirates can now make perfect copies of software and hand them out to their friends, sell them at weekend computer trade shows or via the Internet. In addition, users are setting up their own Web sites allowing the illegal distribution of software and digital content to a global audience.

Pirate sites are now not only found on Web sites, but also on hotline servers, online auction sites, IRC, newsgroups and through e-mail solicitations. SIIA has also seen a jump in the number of cases of e-mail and "snail mail" solicitation cases, where a pirate offers thousands of dollars worth of software for only a few hundred dollars. The professional pirates in these cases "burn" or record these titles onto blank, recordable CDs. They then send out mass e-mail or direct mail solicitations to sell the software copies that they have manufactured.

SIIA was involved in a recent case of direct mail solicitation where the infringer was offering roughly \$15,000 worth of software on a set of CDs for only a few hundred dollars. The ease of duplication, coupled with the ease of downloads from the Internet through DSL and cable modem connections, means that federal law enforcement agencies now face numerous new and challenging avenues of trafficking pirated software.

SIIA's Fight Against Software Piracy At Home

Over the past several years, the U.S. government has taken an increasingly aggressive stance with regard to intellectual property protection and software piracy in particular. SIIA has developed an ongoing relationship with the Department of Justice, particularly the FBI, in addressing the problem of software piracy both in the physical world and on the Internet. SIIA has assisted federal and state authorities in investigating and taking action against all types of infringers, including retailers and trade show exhibitors who offer counterfeit software for sale.

SIIA helps law enforcement by gathering evi-

dence, evaluating evidence seized by police and providing economic loss-impact statements to show the damage that software piracy is doing to a sector that is now the largest contributor to the U.S. Gross Domestic Product (GDP).

SIIA will continue to help federal and local law enforcement in their ongoing efforts to curb the increasing rates of software piracy.

SIIA's Commitment to the Fight Against Software Piracy Abroad

In 1985, SIIA began a comprehensive, industry wide effort to fight software piracy. Today SIIA conducts a wide range of anti-piracy activities, including litigation, end user education and the development of software management tools in the Americas, Europe and Asia. SIIA conducts these activities itself or in conjunction with many anti-piracy organizations that work with SIIA on a regular basis.

SIIA also works to promote adequate and effective protection and enforcement of intellectual property around the world. On issues affecting the global growth of the software industry, SIIA has maintained a strong and consistent voice, calling for:

- protecting and enforcing intellectual property rights of software publishers and developers around the world and on the Internet;
- opposing tariffs and other trade barriers that impede access by software companies to markets in Europe, Asia-Pacific and Latin America;
- seeking and supporting action against software piracy by governments and international organizations such as the World Intellectual Property Organization and other non governmental organizations;
- alerting software developers and publishers to high rates of software piracy and working with them on safeguarding their intellectual property rights through contracts, government registration, litigation and public policy; and
- seeking commitments by governments throughout the world to use only legal software.

To ensure software companies have the legal tools they need to fight worldwide software piracy, SIIA measures national laws and regulations against benchmarks for protection and enforcement, works with officials from the Office of the U.S. Trade

Representative and other executive branch and congressional officials to correct deficiencies in legal regimes and enforcement and directly lobbies foreign governments and international organizations for improvements in the intellectual property protections afforded to computer software.

SIIA's Benchmarks for Intellectual Property Rights

1. Substantive protection and enforcement of copyrights, patents and trademarks in computer software at least as high as that required by the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs) or, if applicable, at higher levels set by multilateral and bilateral agreements.
2. Specific legal authority for the procedural tools and remedies needed by private parties and government to enforce intellectual property rights in computer software, such as ex parte searches and seizures of allegedly infringing goods and items of manufacture, temporary restraining orders, preliminary and final injunctions and monetary recovery.
3. Criminal penalties, including imprisonment, that are substantial enough to deter counterfeiting and commercial-scale infringement by manufacturers, distributors and end users.
4. Demonstrated commitment by national governments and their subdivisions to the protection and enforcement of intellectual property rights in computer software, including:
 - (a) Providing educational programs and publicizing enforcement efforts to reduce piracy rates;
 - (b) Cooperating with the U.S. government and trade associations in enforcement efforts;
 - (c) Ceasing the use of illegally copied software in all government agencies, including educational institutions;

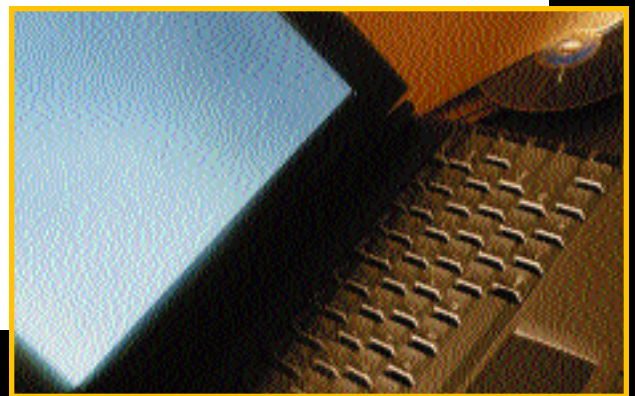
(d) Prosecuting selected high-profile criminal software infringers, including manufacturers and end users, and taking steps to close "software pirate bazaars" openly selling illegally copied software.

The American Perspective

Software piracy is a severe problem in the United States. Piracy of PC business applications in the United States during 1999 resulted in software publishers suffering losses of more than \$3.6 billion in retail sales. Since 1994, business software pirated in the United States has cost publishers more than \$17.7 billion.

Piracy is committed between friends and co-workers or by businesses through illegal rental, counterfeiting or via the Internet. More than just the largest software publishers are affected. Sixty percent of SIIA's member companies have annual revenues of less than \$2 million. Piracy in the United States and abroad seriously damages these small American companies' abilities to compete successfully in the global marketplace and develop the next generation of innovative software.

Software pirates can single-handedly destroy the revenue stream of small companies that have successfully fought to carve out a niche in the industry. Without this revenue stream, these small companies lack the resources for development of new software innovations, decreasing the chances of making a profit. The inevitable result is that these small companies often become economically unstable and often "go under," all because software pirates have decided to steal their software and make it available to others.



Country Detail: Software Piracy Revenue and Losses, 1997 -1999

	Piracy Rates			Piracy Losses		
	1997	1998	1999	1997	1998	1999
WESTERN EUROPE						
Austria	40%	38%	36%	\$41,620	\$51,164	\$66,929
Belgium/Luxemb.	36%	35%	36%	\$51,485	\$53,401	\$77,371
Denmark	32%	31%	29%	\$45,787	\$42,069	\$59,184
Finland	38%	32%	30%	\$37,754	\$36,126	\$50,594
France	44%	43%	39%	\$407,900	\$425,205	\$548,408
Germany	33%	28%	27%	\$508,884	\$479,367	\$652,379
Greece	73%	74%	71%	\$44,546	\$55,385	\$67,708
Ireland	65%	56%	51%	\$46,847	\$60,986	\$117,892
Italy	43%	45%	44%	\$271,714	\$356,879	\$421,434
Netherlands	48%	45%	44%	\$195,098	\$195,778	\$264,400
Norway	46%	40%	37%	\$104,337	\$72,452	\$87,568
Portugal	51%	43%	47%	\$40,991	\$36,109	\$49,920
Spain	59%	57%	53%	\$167,288	\$235,100	\$247,650
Sweden	43%	38%	35%	\$127,051	\$119,073	\$131,358
Switzerland	39%	33%	33%	\$92,898	\$76,471	\$107,068
UK	31%	29%	26%	\$334,527	\$464,771	\$679,506
TOTAL W. EUROPE	39%	36%	34%	\$2,518,726	\$2,760,337	\$3,629,371
EASTERN EUROPE						
Bulgaria	93%	90%	80%	\$13,171	\$17,746	\$11,245
CIS - less Russia	92%	93%	90%	\$44,276	\$47,477	\$43,520
Czech	52%	45%	42%	\$51,972	\$43,261	\$36,897
Hungary	58%	57%	52%	\$25,488	\$38,465	\$37,262
Poland	61%	61%	60%	\$107,625	\$142,484	\$164,914
Romania	84%	86%	81%	\$15,297	\$21,530	\$12,132
Russia	89%	92%	89%	\$251,837	\$273,055	\$165,515
Slovakia	58%	50%	46%	\$17,018	\$11,241	\$9,653
Slovenia	76%	73%	70%	\$9,198	\$12,223	\$10,366
Other Eastern Europe	62%	57%	52%	\$25,474	\$32,532	\$13,708
TOTAL E EUROPE	77%	76%	70%	\$561,355	\$640,014	\$505,213
LATIN AMERICA						
Argentina	65%	62%	62%	\$105,194	\$123,786	\$192,001
Bolivia	88%	87%	85%	\$3,853	\$4,898	\$5,059
Brazil	62%	61%	58%	\$394,994	\$366,688	\$392,031
Chile	56%	53%	51%	\$33,147	\$39,451	\$58,479
Columbia	62%	60%	58%	\$65,085	\$83,615	\$61,843
Costa Rica	74%	72%	71%	\$7,064	\$8,392	\$11,545
Dominican Republic	76%	73%	72%	\$7,647	\$9,019	\$15,267
Ecuador	75%	73%	71%	\$13,236	\$15,619	\$25,142
El Salvador	89%	87%	83%	\$10,419	\$12,949	\$16,697
Guatemala	86%	85%	80%	\$7,867	\$9,357	\$15,580
Honduras	78%	77%	75%	\$3,468	\$4,254	\$6,280
Mexico	62%	59%	56%	\$133,102	\$147,138	\$133,964
Nicaragua	83%	81%	80%	\$5,010	\$6,144	\$6,773
Panama	72%	70%	66%	\$5,859	\$7,004	\$12,832
Paraguay	87%	85%	83%	\$5,029	\$6,371	\$8,198
Peru	66%	64%	63%	\$31,017	\$37,462	\$27,210
Puerto Rico	49%	49%	48%	\$18,826	\$22,874	\$24,956
Uruguay	74%	72%	70%	\$13,613	\$16,109	\$19,608
Venezuela	64%	62%	60%	\$54,905	\$68,298	\$56,823
Other Latin America	75%	72%	72%	\$58,658	\$56,081	\$37,351
TOTAL LATIN AMERICA	64%	62%	59%	\$977,994	\$1,045,506	\$1,127,639

Country Detail: Software Piracy Revenue and Losses, 1997 -1999

	Piracy Rates			Piracy Losses		
	1997	1998	1999	1997	1998	1999
NORTH AMERICA						
US	27%	25%	25%	\$2,779,673	\$2,875,185	\$3,191,111
Canada	39%	40%	41%	\$294,593	\$320,636	\$440,101
TOTAL US/CANADA	28%	26%	26%	\$3,074,266	\$3,195,821	\$3,631,212
ASIA/PACIFIC						
Australia	32%	33%	32%	\$129,414	\$192,237	\$150,390
China	96%	95%	91%	\$1,449,454	\$1,193,386	\$645,480
Hong Kong	67%	59%	56%	\$122,169	\$88,627	\$110,190
India	69%	65%	61%	\$184,664	\$197,333	\$214,557
Indonesia	93%	92%	85%	\$193,275	\$58,756	\$42,106
Japan	32%	31%	31%	\$752,598	\$596,910	\$975,396
Korea	67%	64%	50%	\$582,320	\$197,516	\$197,269
Malaysia	70%	73%	71%	\$82,552	\$79,268	\$84,154
New Zealand	34%	32%	31%	\$20,284	\$21,758	\$19,656
Pakistan	88%	86%	83%	\$20,395	\$22,667	\$18,913
Philippines	83%	77%	70%	\$49,151	\$31,138	\$33,163
Singapore	56%	52%	51%	\$56,599	\$58,262	\$61,758
Taiwan	63%	59%	54%	\$136,850	\$141,274	\$122,946
Thailand	84%	82%	81%	\$94,404	\$48,613	\$82,184
Vietnam	98%	97%	98%	\$10,132	\$10,328	\$13,106
Other Asia/Pacific	83%	74%	71%	\$31,974	\$16,739	\$20,262
TOTAL ASIA/PACIFIC	52%	49%	47%	\$3,916,236	\$2,954,812	\$2,791,531
MIDDLE EAST/AFRICA						
Bahrain	89%	89%	82%	\$3,576	\$3,012	\$6,021
Cyprus	68%	68%	67%	\$1,809	\$1,518	\$3,345
Israel	54%	48%	44%	\$57,060	\$63,239	\$72,487
Jordan	80%	80%	75%	\$1,883	\$1,584	\$3,276
Kuwait	88%	88%	81%	\$7,889	\$6,644	\$13,200
Lebanon	93%	93%	88%	\$1,322	\$1,119	\$2,059
Malta	64%	63%	58%	\$1,299	\$1,090	\$2,220
Mauritius	77%	78%	70%	\$1,070	\$902	\$1,263
Oman	93%	93%	88%	\$5,682	\$4,784	\$9,780
Qatar	87%	87%	80%	\$2,760	\$2,325	\$4,451
Reunion	59%	59%	54%	\$1,232	\$1,036	\$1,458
Saudi Arabia	74%	73%	64%	\$46,156	\$38,768	\$39,900
Turkey	84%	87%	74%	\$64,306	\$55,823	\$98,257
UAE	50%	49%	47%	\$4,420	\$3,637	\$7,624
Other Middle East	73%	73%	69%	\$5,538	\$4,661	\$19,103
TOTAL MIDDLE EAST	72%	69%	63%	\$206,003	\$190,140	\$284,445
AFRICA						
Egypt	85%	85%	75%	\$12,890	\$10,858	\$33,197
Kenya	72%	72%	67%	\$302	\$254	\$372
Morocco	72%	72%	64%	\$4,559	\$3,829	\$5,267
Nigeria	72%	72%	67%	\$2,509	\$2,107	\$2,951
South Africa	48%	49%	47%	\$69,833	\$94,241	\$84,149
Other Africa	71%	70%	67%	\$95,414	\$78,591	\$67,811
TOTAL AFRICA	60%	58%	56%	\$185,507	\$189,881	\$193,747
TOTAL MDL. EAST/AFR.	65%	63%	60%	\$391,509	\$380,020	\$478,192
TOTAL WORLD	40%	38%	36%	\$11,440,086	\$10,976,510	\$12,163,159

The use of business application software to carry out day-to-day business functions is now almost universal. Even nations slowly emerging into the new global economy – and often struggling to develop even a basic business infrastructure – are using PC hardware and business application software to achieve a technological foothold in a fast-changing world.

Unfortunately, in many countries with developing economies, demand for software is being met by piracy – not by publishers. American software publishers are unable to compete with counterfeit operations that duplicate their programs and distribute them directly to consumers on street corners and shops throughout the world at prices often as low as \$2.

Software companies invest in technology to achieve a competitive advantage in the marketplace. The investment in research and development has proved a significant factor in the continued success of the U.S. software industry. Continued expansion of software products into international markets also has played a key role in the U.S. software industry's success and could perform the same role in the economies of other countries if adequate intellectual property protections were in place.

Piracy inhibits – and in most cases prevents – local software developers from being credited with the development of their product or paid for their intellectual property. When foreign nationals develop a breakthrough product, counterfeiters attack them just as swiftly and severely as they do American products.

Although some argue that lower levels of personal income justify software piracy, this is misleading. In most developing countries, computer software is only used by a relatively small group of individuals and organizations affluent enough to purchase computers, not by the average citizen. More significantly, if individuals and organizations can afford to buy computer hardware, why shouldn't they be expected to purchase legitimate copies of software to run on that hardware?

Arguments citing the industry's infancy, fragility or strategic importance are secondary, at best, because governmental initiatives in support of a local software industry so often lead to protectionism, lack of competition and technological stagnation.

Software piracy prevents natural allocation of resources in an efficient manner and calls for targeted governmental intervention. Governments can play a significant role in shaping an environment friendly to

software industry development by protecting intellectual property, encouraging research and development (R&D) through the introduction of R&D tax credit systems and reducing taxes on capital gains.

SIIA works with the U.S. government, foreign governments and international organizations around the world to protect intellectual property in international markets. The Special 301 provision of the Omnibus Trade and Competitiveness Act of 1988 authorizes the U.S. Trade Representative (USTR) to prepare lists of Priority Foreign Countries that deny adequate and effective protection of intellectual property rights or deny fair and equitable market access to U.S. firms and individuals relying on intellectual property protection. The lists inform the administration of nations considered priority targets for future and ongoing trade negotiations or possible trade sanctions.

In February 2000, SIIA Recommended the Following 26 Countries to the USTR for Special 301 Consideration:

Section 306 Monitoring – China
Priority Watch List – European Union, Greece, Guatemala, India, Indonesia, Israel, Macau, Pakistan, Philippines, Russia, Turkey and Vietnam.

Watch List – Argentina, Brazil, Ireland, Korea, Malaysia, Mexico, Poland, Romania, Saudi Arabia, Singapore, Taiwan, Thailand and Uruguay.

SIIA fully supports the USTR's efforts to open and protect international markets for legitimate sales of software and to combat the theft of intellectual property in these markets. Continued, vigorous action by the U.S. government is necessary to protect the intellectual property lifeblood of the American and international software industries.

Comparisons of the Size and Geographic Distribution of Software Piracy

The data contained in this report show that the countries studied have very different software piracy rates and dollar losses. These differing rates and losses are due to a number of factors. In general, the emerging economies of Asia and the Americas have higher rates of



piracy, even though their smaller markets result in lower total dollar losses than in other countries. This is due to simple mathematics: 25 percent of \$10 billion is a much larger number than 75 percent of \$1 billion. Thus, the United States, the largest personal computer software market in the world, leads the world in piracy losses. SIIA estimates that \$3.2 billion worth of personal computer business application software was pirated in the United States in 1999. This represents about 25 percent of the total world losses.

In 1999, Vietnam had the dubious distinction of carrying the highest piracy rates in the world – 98 percent for personal computer business applications. This is the sixth year in a row that Vietnam has had this distinction. China’s rate declined slightly from 95 percent in 1998 to 91 percent this year. Rates such as these earn markets the epithet of “one-copy countries,” meaning piracy is so rampant that one legitimate copy of software could serve the entire market, and severely inhibit free movement of software products and services. Neither foreign producers nor domestic start-ups can establish a legitimate market for their products when the competition is selling for prices that bear no relation to the actual costs of development.

SIIA calls on all governments to join USTR’s initiative for legal software use by making the commitment to use only legal software in government entities and operations and by establishing comprehensive and accountable software asset management practices.

SIIA’s Challenge to Governments

For 2000, SIIA calls on foreign governments to do their part in the fight against software piracy by taking the following steps:

- Meet the challenge of the U.S. Trade Representative by making a commitment to:
 - (i) use only legal software in government agencies and state-owned enterprises, (ii) budget the funds needed to license legal software and (iii) stay legal by implementing accountable software asset management practices.
- Make effective enforcement efforts against all forms of software piracy a reality by complying with the obligations of the TRIPs Agreement.
- Ensure that computer software is no less protected on the Internet than on the street by promptly joining the WIPO Copyright Treaty, enacting legislation to meet the treaty’s obligations and effectively enforcing those laws without undue delay.

SIIA is prepared to help countries fight software piracy with its Certified Software Manager (CSM) Software Asset Training Program, now available for the United States, Canada, China, Hong Kong, Singapore, Australia and New Zealand, and with its experience in implementation of the TRIPs Agreement and the WIPO Copyright Treaty.



As noted previously, SIIA recommended 26 countries and territories to the USTR for Special 301 consideration. As this report shows, more than half the business software in use last year in each of these countries and territories was pirated. That figure is eclipsed in two countries – China and Vietnam – where more than 90 percent of the business software in use is pirated. In all, business software piracy in these 26 countries and territories cost U.S. software publishers nearly \$3 billion in 1999, and piracy of software for Internet, education, reference and entertainment is thought to have cost hundreds of millions – perhaps billions – more. Although estimated dollar losses to software piracy increased in 1999, the most likely explanation is increased use of software. Because the software piracy rate was virtually unchanged in many of these jurisdictions, the increase in losses may well represent a hiccup – possibly due to Year 2000 (Y2K) preparation – rather than real change in underlying behavior toward piracy. Protecting copyrighted software from theft requires continued vigilance and effort.

Western Europe

Europe is the largest regional software market outside the United States. It is also the market most like the United States in terms of software use patterns and computer penetration rates. Within Europe, striking differences remain in economic development and software piracy rates. The share of software pirated ranges from a high of 71 percent in Greece to a low of 26 percent in the United Kingdom. The largest computer markets – Germany, the United Kingdom and France – had the

Western Europe

Highest Rate:

Greece: 71% piracy rate

Spain: 53% piracy rate

Average European rate: 34%

Revenue loss for Western Europe: \$3.6 billion

highest dollar losses in the region. All of these countries had dollar losses due to software piracy in excess of \$500 million. In comparison, Greece, which has the highest piracy rate in the region of 71 percent, had \$67.7 million in software piracy losses due to its smaller market.

Although one might expect piracy to be greater in countries with low per-capita income, no country in Europe has a low enough per-capita GDP to explain the high rates of piracy seen in some European nations. Piracy losses in Western Europe rose modestly in 1999 – from \$2.76 billion in 1998 to \$3.63 billion in 1999. The average piracy rates in 1999 for all of Western Europe were 34 percent, a nominal decline from 36 percent in 1998.

Central Europe

As an emerging market for software, Central Europe has great potential – but only if strong intellectual property protection is enacted and enforced. With 1999 piracy rates above 80 percent in four of 10 countries in this area, Central Europe cannot be considered a

Central Europe

Highest Rate:

Other former Soviet states: 90% piracy rate

Russia: 89% piracy rate

Average Central European rate: 70%

Revenue loss for Central Europe: \$505 million

viable market for software unless improved protection is implemented. Some notable exceptions include the Czech Republic and Slovak Republic, with rates at only 38 and 46 percent, respectively.

Because of Russia's high level of software piracy (89 percent), its lack of effective enforcement and its continued lack of retroactive protection for computer programs prior to the adoption of the 1993 Copyright Act revisions in Russia, SIIA recommended the USTR place Russia on the Priority Watch List.

The Czech Republic, Poland and Hungary are the strongest legal software markets in Central Europe. These economies have been relatively stable for the past few years, have avoided war and have already survived hyperinflation and the adjustment from communism to a market economy.

Mexico, Central & South America

The countries of the Americas are a study in contrasts, both economically and in their use of personal computer software. Brazil and Mexico, along

Mexico, Central & South America

Bolivia: 85% piracy rate
Guatemala: 80% piracy rate
Average Central & South American piracy rate: 59%
Revenue loss for Central & South America: \$1.1 billion

with most of Central and South America, have high piracy rates, along with per-capita incomes that are only about 10 percent as large as those of the United States and Canada.

Central and South America represent a rapidly expanding growth market for PC software. Most individual markets are still rather small, but their software sales growth rates are, for the most part, encouraging. Brazil and Mexico, followed by Argentina and Colombia, are the largest single markets in the region and have been for all of the 1990s.

Unfortunately, piracy rates in the region remain quite high – virtually all in excess of 60 percent. With piracy rates at around 60 percent and with the largest software markets, Argentina, Brazil and Mexico also provide nearly two-thirds of the region's piracy losses.

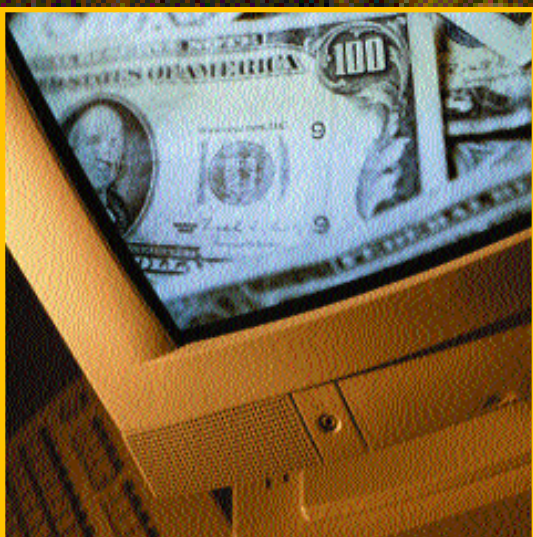
Mexico's revenue growth has been plagued by currency crises, which can contribute significantly to changes in shipment value for any international market. Fifty-six percent of all software in Mexico is pirated, resulting in revenue losses of nearly \$134 million. Mexico has been slow to improve enforcement efforts against software piracy and to institute judicial and law enforcement reform related to the enforcement of intellectual property rights.

North America

The North American software market is still a remarkable engine of growth. PC software continues to supply increased functionality and efficiency to businesses, homes, and individuals. PDAs, or personal digital assistants, wireless phones and other devices join the list of tools that consumers demand – all powered by software. Over 80 percent of U.S. businesses currently rely on PCs in their day-to-day

North America

Canada: 41% piracy rate
United States: 25% piracy rate
Average North American rate: 26%
Revenue loss for North America: \$3.6 billion





operations, and that number continues to grow. The United States represents the largest software market in the world, with business PC application sales of more than \$9 billion in 1999. The Canadian market is necessarily smaller, due to its much smaller population, but it is growing at a higher rate than the United States.

North America has historically had the lowest regional piracy rate – one that has decreased steadily over the years. Due to the size of its software markets, however, North America still accounts for by far the largest regional global piracy losses. Forty-four percent of worldwide revenue lost to piracy in 1999 was due to North American activity. Obviously, software piracy remains a large problem in North America.

Middle East & Africa

The Middle East and Africa comprise a large geographic area containing some extremely wealthy and some extremely poor nations and great differences in the use of information technology. Because the region

Middle East & Africa

Lebanon & Oman: 88% piracy rate

Bahrain: 82% piracy rate

Average Middle Eastern/African piracy rate: 63%

Revenue loss for Mideast/Africa: \$478 million

encompasses many barely emerging markets, SIIA's information on the region as a whole is incomplete. South Africa is the largest software market in the region, a distinction it has maintained for as long as SIIA has been tracking international sales.

Israel has developed a strong domestic software industry and has successfully exported that software internationally. Israel's copyright law, however, is in dire need of revision to ensure that there is substantive copyright protection for computer programs – the principal reason why SIIA named Israel to the Special 301 Priority Watch List. The Israeli government also needs to increase its enforcement efforts and penalties for pirating software.

Turkey amended its copyright law in 1995 to extend protection to computer programs. Since 1995, software piracy rates have moved from 90 percent to 74 percent in 1999. Turkish software piracy cost U.S. software publishers more than \$98 million in 1999.

On the whole, growth rates for the region have been quite strong for the past few years – consistently higher than the world average. This is typical of developing markets, where computerization expands to assist businesses in increasing their efficiency as increasing wealth permits specialization and participation in the world economy.

Asia-Pacific

Asia-Pacific is also a region of vast economic extremes. Japan has great economic strength as well as a high level of computer use and moderate software piracy. China, India, Malaysia and Thailand have per-capita GDP rates significantly lower than those of more prosperous nations of the region, but the booming economies of these trading “tigers” belie any justification for software piracy rates ranging from 60 percent to more than 95 percent.

Of the Asia-Pacific markets for which SIIA is able to develop piracy estimates, only Australia, Japan and

New Zealand had piracy rates below 50 percent. Software companies lost an astounding \$2.8 billion to Asian pirates, with an average regional piracy rate of 47 percent.

Japan is the largest single software market outside the United States and is still showing quite rapid expansion. Piracy in Japan cost software publishers \$975 million last year. Japan has a thriving domestic software and hardware industry, primarily devoted to proprietary-platform products, and these losses include damage to Japanese producers, as well as U.S. publishers.

The Republic of Korea's (South Korea) 50 percent piracy rate for business software, with \$197 million losses in 1999, allowed infringers to

make millions of illegal copies of software. Korea's domestic industry, with nearly half of all sales in the market, suffers heavy losses compared with many local publishing industries. Similarly, Indonesia – with one of the highest software piracy rates in the world –

remains a significant concern. Until the Indonesian government takes concerted action against this problem, virtually all of its software demands will be met by pirated products, as is the case today.

Although the Chinese government deserves credit for taking action to close pirate CD-ROM factories and for imposing credible criminal penalties on the parties responsible, software piracy remains rampant in the workplace. Counterfeit software can still be purchased in retail stores, and criminal prosecutions against pirate factory owners and large-scale pirate distributors are inconsistent and sporadic. Piracy losses in China for 1999 were \$645 million, with the rate falling to 91 percent from 95 percent in 1998.

Despite recently enacted intellectual property legislation, most Asian countries have not yet implemented strong enforcement practices, allowing copyright infringers to continue pirating software. Sources indicate widespread duplication and distribution of counterfeit CD-ROM software is occurring in Hong Kong, but SIIA has worked closely with U.S. and Hong Kong customs officials to address this problem.

Asia-Pacific

Vietnam: 98% piracy rate

China: 91% piracy rate

Average Asian-Pacific piracy rate: 47%

Revenue loss for Asia-Pacific: \$2.8 billion



A Final Word

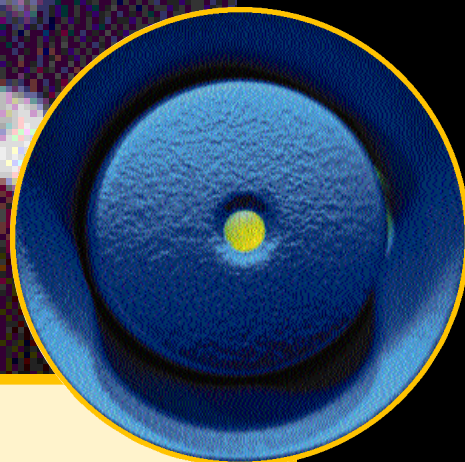
There is no evidence – either in this report or elsewhere – that software piracy will be eliminated anytime in the foreseeable future. SIIA acknowledges that many countries identified have made efforts to improve intellectual property protection in computer software. For the countries identified in this report, however, the high rates of software piracy and dramatic losses to U.S. software developers demonstrate that much remains to be done. There is evidence that continuing education and enforcement efforts can – and do – make a difference. In the United States, for example, the level of piracy has been reduced from 48 percent in 1989 to 25 percent in 1999.

Thus, we have learned that decreasing software piracy rates requires the combined efforts of policy-makers, software developers and publishers, businesses, journalists and individuals. As long as software piracy remains, there will be fewer jobs, less research and development, increased costs and lower standards of living.

“SIIA’s Report on Global Software Piracy” or portions thereof may be reproduced for personal, noncommercial or not-for-profit use only provided copies bear the copyright notice “©2000 Software & Information Industry Association,” are attributed to the Software & Information Industry Association (SIIA) and are not altered in such a way to prejudice the honor or reputation of SIIA. Other uses require separate permission from SIIA.

The piracy loss and rate estimates upon which this report is based are the result of a commissioned methodology and study by International Planning Research Group (IPR). SIIA and the Business Software Alliance jointly commissioned IPR to develop and implement a methodology resulting in data both groups would jointly release annually.

For additional copies, contact SIIA’s customer service department,
(202) 452-1600, ext. 349, or orders@siaa.net.
For additional information on SIIA, please go to www.siaa.net



The **Software & Information Industry Association (SIIA)** is the principal trade association of the software code and information content industry. SIIA represents over 1,000 high-tech companies that develop and market software and electronic content for business, education, consumers, the Internet and entertainment. SIIA member companies account for 85 percent of U.S. revenue for packaged and online software. Hundreds of these companies look to SIIA to protect their intellectual property rights around the world. SIIA combines strong anti-piracy education and enforcement efforts through such programs as its U.S. and Canadian anti-piracy hotline (1-800-388-7478), an online service for piracy reports (www.sii.net/piracy/report.htm), the Certified Software Manager (CSM) course, SPAudit, KeyAudit, videos, posters and other awareness materials. Information on SIIA and its wide range of activities can be found at www.sii.net.

SIIA was formed on January 1, 1999, as a result of a merger between the Software Publishers Association (SPA) and the Information Industry Association (IIA).



1730 M St. NW, Suite 700
Washington, DC 20036-4510
202.452.1600
Fax: 202.223.8756

www.sii.net