Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

WHITE PAPER

The Dangerous World of Counterfeit and Pirated Software

How Pirated Software Can Compromise the Cybersecurity of Consumers, Enterprises, and Nations ... and the Resultant Costs in Time and Money

Sponsored by: Microsoft

John F. Gantz
Joe Howard
Richard Lee
Harish N. Taori
Ricardo Villate
Christian A. Christiansen
Albert Wang
Christian Lachawitz
Thomas Vavra
Rich Rodolpho
Attaphon Satidkanitkul
Ravikant Sharma
Alejandro Florean
Stephen Minton
Marcel Warmerdam

March 2013

IN THIS WHITE PAPER

This White Paper presents the results of an investigation by IDC into the prevalence of malicious code and unwanted software — such as viruses, Trojan horses, keystroke-capturing software, authentication backdoors, and spyware — in pirated software and on the Web sites and peer-to-peer (P2P) networks where such software is found. It updates and extends a study conducted in 2006.

It also quantifies the cost in time and money to individuals and enterprises dealing with the effects of malware found in pirated software using information from a 10-country survey of 1,104 consumer respondents, 973 business user respondents, and 268 CIO/IT manager respondents.

Note: What's the difference between pirated software and counterfeit software? In this document, "pirated software" refers to software that is improperly licensed or not licensed at all, and "counterfeit software" refers to a subset of pirated software that is deliberately presented as genuine when it is not. In this White Paper, we use either term when appropriate.

INTRODUCTION

Do you know where your computer software has been? In a world where criminal organizations have been tracked to both the creation of counterfeit software *and* the creation of all sorts of malicious code used in cyberattacks, perhaps you should.

Consider this:

- The market for credentials and other information stolen by cyberthieves has been sized at $114 billion (2011),[1] enough to create a multibillion-dollar market for tools to enable cybertheft. A decent keylogger — malware that tracks keystrokes to gather passwords and account information — can cost as little as $25 on an auction market used by cyberthieves. Botnets sell at $100–200 per 1,000 infections, depending on location.[2] There is a whole subterranean industry selling toolkits (with code names like Zeus, Citadel, Ice IX, and SpyEye) to cybercrooks who then create malware with equally arcane names like "police ransomware," "spear phishing email," "LuckyCat," "Fakem Rat," or "HeartBeat APT."[3]
- According to BSA | The Software Alliance, 42% of all PC software packages installed in the world in 2011 were pirated. However, in 50% of the countries studied, more than 60% of the software was pirated. IDC estimates that at least 80% of pirated software is counterfeit — so at least a third of PC software is counterfeit.
- The path to *obtaining* and then *using* such counterfeit software is fraught with security danger as well. If the software itself doesn't have malware in it, the Web sites and P2P networks from which it is often downloaded can infect user PCs during the download process. And to activate counterfeit software, you will often need some authentication codes. Counterfeit versions of these codes are available online — but, again, at highly infectious locales.
- What's more, our research and research conducted by Microsoft and other third parties show that pirated software can end up on user and enterprise PCs (e.g., coming in preinstalled software on PCs) without the user knowing it isn't genuine. Often this software is infected with malware on arrival.

In other words, your chances of encountering malicious code in counterfeit software are high — whether you know it's counterfeit or not. And the cost to individuals, enterprises, and even governments and nations can be high: lost time, money, data, and patience.

[1] "Stolen Credit Cards Go for $3.50 at Amazon-Like Online Bazaar," Bloomberg, December 20, 2011.
[2] BITS Financial Services Roundtable, *Malware Risks and Mitigation Report*, June 2011.
[3] Taken from a list of research papers at Trend Micro's Web site**.**

In 2006, IDC completed a similar study and corresponding White Paper sponsored by Microsoft, but that study focused largely on the United States.[4]

In this study, we have updated that previous work by taking a 360-degree view of the security risks in obtaining and using pirated software — whether bought as physical media, downloaded off the Internet, or obtained through the distribution channel inadvertently. We also have added more geographic reach to our scope, with a special emphasis on China.

In addition, we augmented our lab work to include testing for malware across multiple geographies and conducted a global survey to assess the actual time and money individuals and enterprises must spend dealing with the security breaches attendant to obtaining and using pirated software.

Differences Between 2006 and 2013

IDC performed a similar but more limited study in 2006. So what is different between then and now?

- Overall we found a somewhat cleaner environment. Back then, 25% of Web sites tried to infect our computers; this time it was 14%. Back then, 33% of CDs/DVDs tested were infected or had vulnerabilities; this time only 14%. Today, browsers are much better at fending off hijackers and redirectors, and search engines are much better at avoiding highly infectious sites.
- However, based on our work on the BSA | The Software Alliance global piracy study, IDC believes that at least three times as much pirated software will be installed this year as in 2006.
- As broadband connections have improved and the number of PCs accessing the Internet has grown — by a factor of 2.2, to be exact — more and more pirated software is coming over the Internet.
- Street market pirated software is getting better — more functional and cleaner – but also harder to find in more and more countries. For instance, in 2006 there was no problem finding counterfeit CDs/DVDs in Russia; this time we didn't find enough to test.
- By all accounts, the threats delivered via malware are worse today than in 2006: more criminal organizations involved, more money and data theft, and more sophisticated attacks and fraud.

EXECUTIVE SUMMARY

- Based on studies by IDC and BSA | The Software Alliance, IDC estimates that a third of PC software in the world is counterfeit. Because of the link between counterfeit software and IT security issues from malware, this poses a danger for consumers, enterprise, and nations.
- In lab tests that included 533 tests of Web sites and P2P networks offering counterfeit software and counterfeit CDs/DVDs, IDC encountered tracking cookies/spyware 78% of the time when downloading software from the Internet and Trojans and other malicious adware 36% of the time. On the CDs/DVDs that were actually installable, we encountered Trojans and malicious adware 20% of the time, in part because sometimes it was necessary to obtain illegal activation keys online.
- In addition, consumers and CIOs/IT managers surveyed told us that software delivered through normal delivery channels often was improperly licensed or infected their PCs with malware. On average, this occurred more than 15% of the time.
- Given these infection rates, if you use pirated software, chances are one in three that in the process of obtaining or using that software, you will encounter dangerous malware.
- As a result of malware from counterfeit software, IDC estimates that consumers worldwide will waste 1.5 billion hours this year dealing with it.

[4] *The Risks of Obtaining and Using Pirated Software*, IDC White Paper, October 2006.

- IDC estimates that the direct costs to enterprises from dealing with malware from counterfeit software will hit $114 billion this year. The potential losses from data breaches could reach nearly $350 billion.

- The dangers from counterfeit software are real. For consumers, it is not just lost time and money to fix the problem but also the risk of lost data and identity theft. For enterprises and governments, it is time and money better spent on other things, lost business and reputation from data breaches, and threats to critical infrastructure.

THE PIRACY LANDSCAPE

There are a number of ways for end users to obtain pirated software.

In addition to violating the terms of a volume license, the most common methods are:

- Downloading the software from Web sites or P2P networks. With modern broadband Internet connections, downloads can take less than an hour.

- Obtaining physical media for sale over the Internet, either from legitimate sites, such as eBay, or from sites that advertise using email, Web site spam, and so on.

- Obtaining physical media in the physical world, such as from street vendors, in kiosks, and sometimes even in computer stores. This could include obtaining copies of counterfeit software from friends.

- Finding it already installed on the PCs or software purchased from distribution channels.

In the first three cases, the software may require counterfeit activation tools to function, which generally entails a trip back to Web sites or P2P networks to obtain.

Based on our survey, IDC believes that, today, most counterfeit software that doesn't simply come with the computer comes over the Internet rather than from street markets. At least that's what consumers told us, as shown in Figure 1.

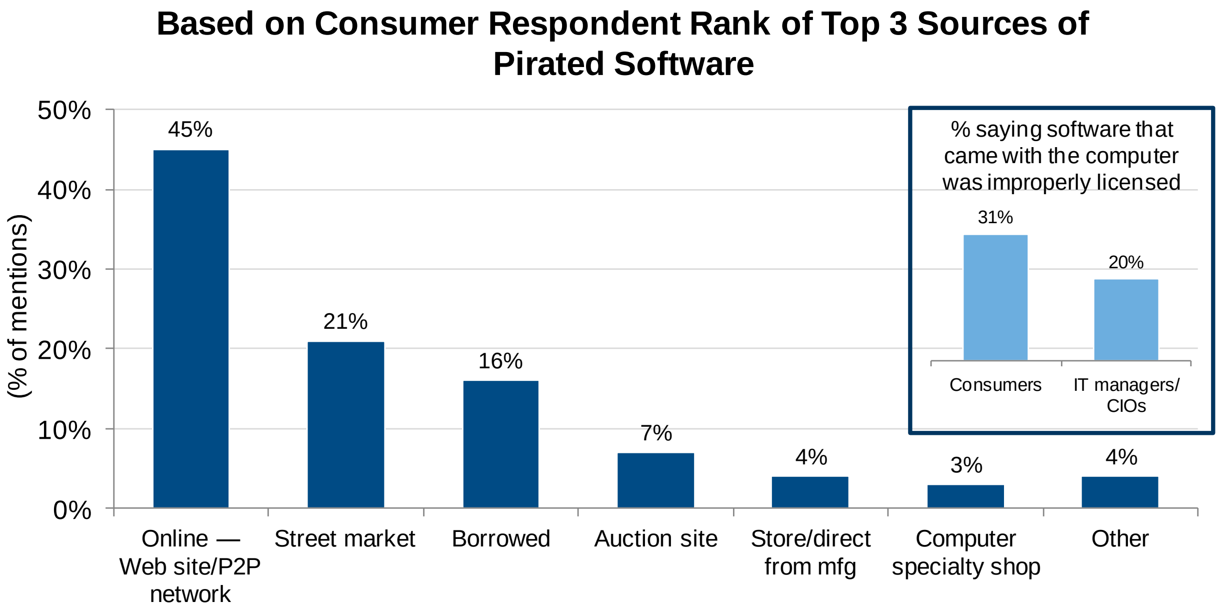
But the picture is murkier than that, as the fourth point in the preceding list indicates. Consumers *and* enterprises told us that a fairly high proportion of pirated software came with the computers they bought, as shown in the inset in Figure 1.[5] Where *that* pirated software came from is unknown. For instance, it could have been installed on the PC by a channel player who bought hardware without software and added it on or by a company that builds PCs from components.

Another indication of that murkiness: The IT managers and CIOs we surveyed told us that of the PCs they had bought in the past three years, 7% showed a different brand when they were booted up than the IT managers and CIOs thought they were buying!

[5] "Microsoft finds new PCs in China preinstalled with malware," *PCWorld*, September 14, 2012.

FIGURE 1

Where Pirated Software Comes From



n = 1,104

Source: IDC's *Dangers of Counterfeit Software Survey*, 2013

The counterfeit software itself can come from any number of sources, including individuals, small teams of hackers, giant shadowy enterprises like The Pirate Bay, and major piracy syndicates like the one taken down by the FBI and Chinese authorities in 2007 where $500 million worth of counterfeit software was seized,[6] or even the Mexican drug cartel known as Familia Michoacana that sells counterfeit software with its own logo on it at more than 150,000 locations in Latin America.[7]

In many cases, the physical counterfeit programs and activation keys are created from Internet downloads copied over and over again and packed for resale in street markets or to be launched into distribution channels that sell PCs with software loaded on them.

[6] "F.B.I. and Chinese Seize $500 Million of Counterfeit Software," *New York Times*, July 25, 2007.
[7] "Familia, 'Pirateria,' and the Story of Microsoft's 'CSI' Unit," InSight Crime, February 10, 2011.

AN INFECTIOUS ENVIRONMENT

Our lab tests map the minefield users must traverse when they obtain and try to use counterfeit software. Consider the following:

- In the search for counterfeit copies of Office on the Internet (across 270 Web sites and P2P networks), we encountered malware just by visiting these sources: tracking cookies and spyware detected on our virtual PCs from 75% of the sites, Trojans and malicious adware at 14%.

- Once we started downloading software, the tracking cookie/spyware installations edged up closer to 78% and Trojan and malicious adware count jumped to 27%.

- However, 60% of the downloaded software didn't come with activation keys, which meant some users had to go back to the download site at least once and sometimes repeatedly to obtain illegal keys. Just one trip back to the Web site/ P2P network sources for keys by those who need them drove the chance of Trojan/adware infection from obtaining an *installable* copy of software to 36%.

- When navigating the sites or downloading software, we developed system performance issues more than 25% of the time. Our testers estimated that more than half the time, either the virtual PCs crashed or the system slowed to the point that it was unusable.

- Of the 155 CDs/DVDs we tested from around the world, we found 30% were not installable — computers froze, software simply wasn't there or wouldn't load, screens went blank — but of those that were installable, 15% ended up infecting our computers with malware.

- Most of the installable CD/DVD-based programs offered either some kind of activation bypass or illegal activation keys; however, 14% required a trip to the Internet to obtain illegal activation keys. That extra trip drives the infection rate of installable programs to 20%.

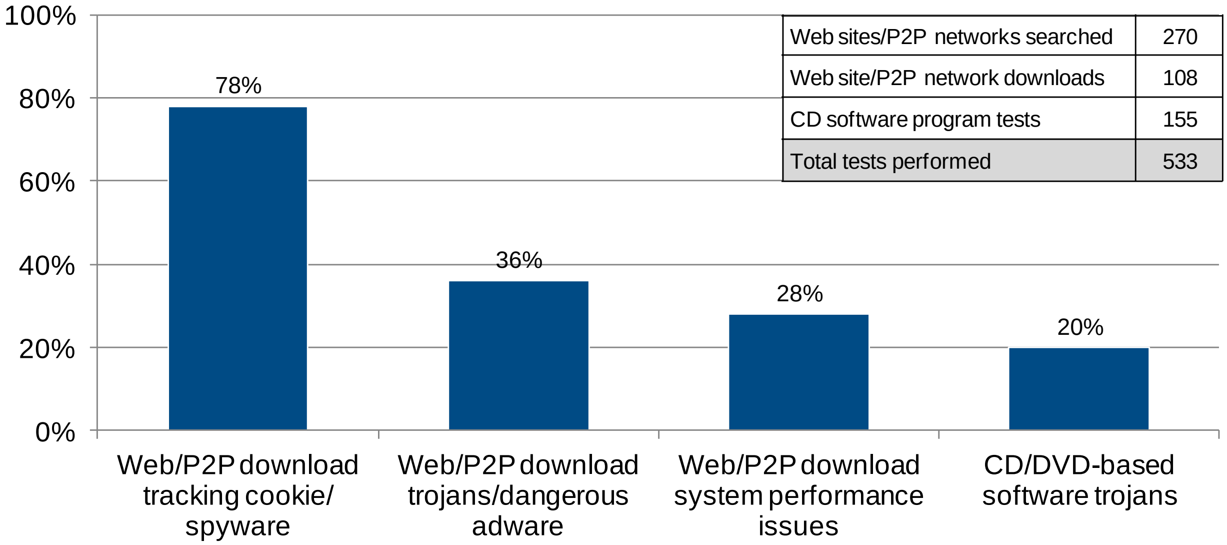
- Most of the CDs/DVDs came with extra software, whether wanted or not, and often the installation process displayed unusual behavior, such as music playing during installation, pop-ups showing up with Web links to dating or pornography sites, or links to other sites known to be potential security threats.

Figure 2 summarizes our lab test findings. Note that infection rates for downloaded software and CD/DVD-based software include the infection caused by the need to download illegal activation keys in some cases. They do *not* account for infections after installation because users may be nervous about installing security updates on counterfeit software.

FIGURE 2

Counterfeit Software Infection Rates

% of Downloaded Programs*/CDs Installing Malicious Code



Web sites/P2P networks searched	270
Web site/P2P network downloads	108
CD software program tests	155
Total tests performed	533

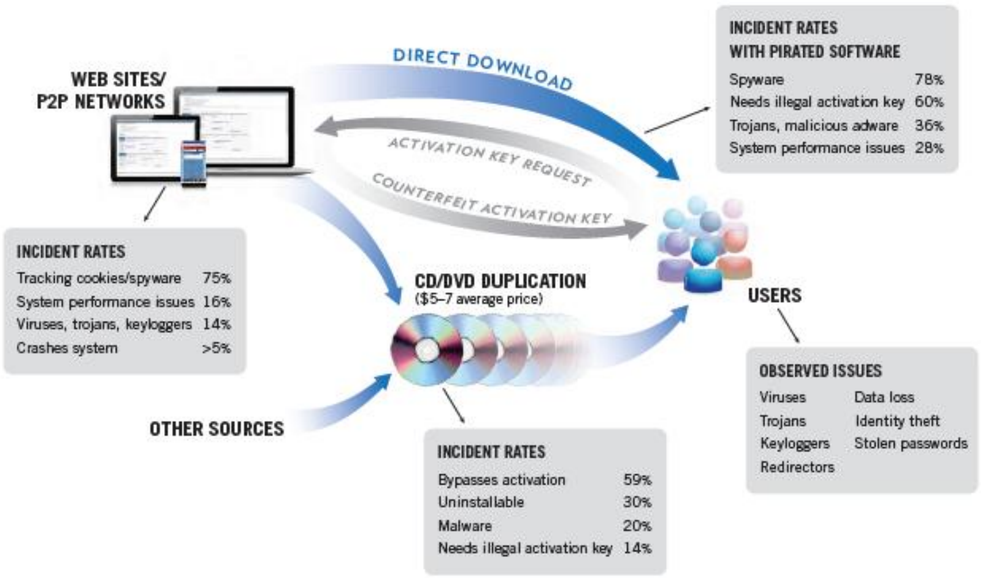
* Infection rate includes malware encountered when returning to the Internet to obtain illegal activation codes.

Source: IDC's *Dangers of Counterfeit Software Survey*, 2013

Figure 3 offers a 360-degree view that depicts how counterfeit software reaches the market and how infectious each step of the process can be.

FIGURE 3

The Dangerous World of Software Piracy



Source: IDC's *Dangers of Counterfeit Software Survey*, 2013

In fact, given the sources of software and the malware rates by source, if you choose to use counterfeit software, you will encounter malware a third of the time. Given piracy rates around the world, that means that installing nearly one in eight PC consumer software packages entails an encounter with malware, one in nine with business PC packages.[8]

[8] Note that we did not say how many PCs might be infected. This is because we have studied only the infection rate per package, not how many counterfeit packages might be on one computer. For analysis purposes, the conservative view is to assume that a 33% (1 in 3) infection rate for counterfeit software packages in a market with a 33% counterfeit software rate (1 in 3) means a 1 in 9 chance of a PC being infected. But the number could be different based on the distribution of counterfeit software packages — many packages to a few PCs, or a few counterfeit packages to many PCs. We believe that the latter is more likely and that if 1 in 9 software packages is infected, the minimum of PCs infected would be 1 in 9.

HOW DANGEROUS IS THIS MALWARE?

Some of the malware we found in the lab tests seemed innocuous enough, as it targeted vulnerabilities that have been addressed by published updates.

On the other hand, research published in 2008 indicated that only 5% of PCs running Windows were doing so with all updates installed.[9] A study by Skype in 2012 indicated that 40% of adults don't always update their systems when prompted, and 25% skip the updates altogether.

In our own survey, we found that 46% of consumers don't install security updates, and 10% of enterprises surveyed had even disabled their automatic security updates.

And we *did* find some nasty malware.

For example:

- Win32.Generic!BT is described by Lavasoft as "a Trojan which extracts from itself another malicious program providing the attacker with unauthorized remote access to the infected computer."
- Bprotector is a Trojan that normally attacks from Web sites, but it can also be inserted into downloadable software. The first thing it does on your system is change system default settings to make it hard to eradicate. It is designed as a door opener for other malware and to allow hackers to take control of your computer. It must be removed manually by professionals.
- iBryte is a browser hijacker that makes it seem like your home page is getting live news feeds but that serves up spam ads. Although this may be just annoying, iBryte can also track your Web browsing habits, gather your personal information, and transmit that information to remote attackers.

What about the code detected by our spyware removal tool, mostly aggregated as "tracking cookies"? How dangerous are they?

It's debatable. Cookies, or small text files that Web sites leave on your computer, can be useful. They remember information about you that helps you log on to familiar Web sites. Tracking cookies are a subset of cookies that also keep track of what Web sites you visit and report that information back to the site that installed them. They can be used to amass information about preferences and target specific advertising campaigns to you.

On the other hand, do you want information about you and your Web site browsing habits available to companies like those that offer pirated software, games, movies, or pornography?

[9] "Keeping your computer up-to-date," BullGuard.

And some of the spyware we ran into didn't seem that tame. GamePlayLabs, for instance, purports to help you in Web browsing but monitors your activities in order to serve you ads. But it is designed, as well, to install and launch other malicious programs on your machine and allow hackers to gain access to your computer. It often shows up in "free" software. Babylon is a browser redirect virus that can hijack your Web browser and redirect search results to unwanted sites. It can be innocuous, but it can also slow down your system and lead you to infected sites.

WHAT DOES THIS MEAN FOR YOU?

If you are a software pirate, the test results speak to the dangers of accessing the kinds of sites you need to obtain counterfeit software or activation tools — the risks of wandering into an unsavory region of cyberspace.

If you are just a law-abiding PC user, the survey results speak to the environmental hazards of software piracy — you may get infected from software you don't know is counterfeit.

The risks that should be balanced against the low price of counterfeit software include:

- **Infection from unwanted code** — running from mild to severe, from a barrage of pop-ups overrunning your computer to keyloggers stealing your banking passwords

- **Degradation of security protection —** from lack of access to security updates to code that disables antivirus programs or personal firewalls from running

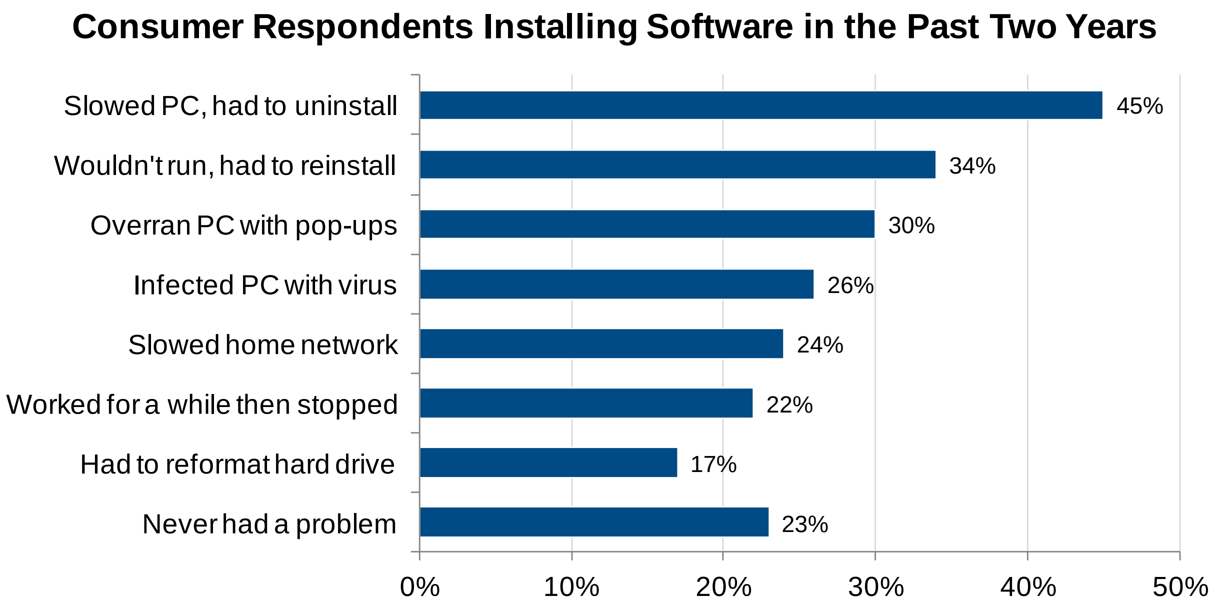
- **Degradation of application performance —** from computer and network slowdowns to complete system crashes, like those we found from time to time in our lab tests

In our survey, consumers indicated clearly that they (1) had experienced security problems with pirated software and (2) knew what they worried about most from those security issues.

Respondents told us that 64% of the people they know have used counterfeit software and have experienced security problems with it. The problems experienced are shown in Figure 4.

FIGURE 4

Problems of Pirated Software



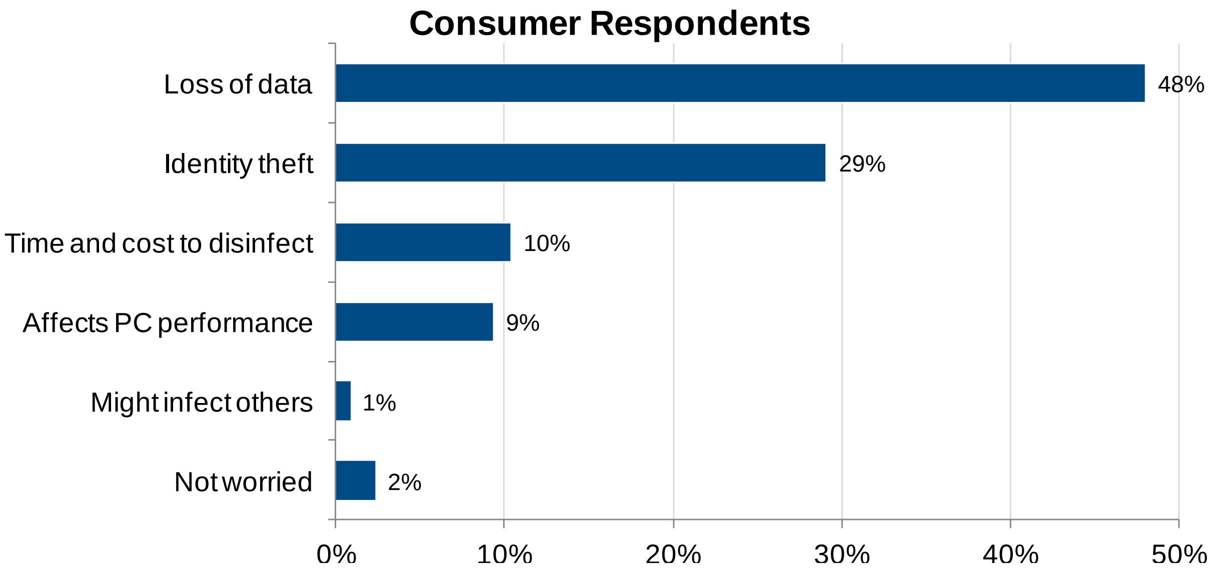
n = 1,104

Source: IDC's *Dangers of Counterfeit Software Survey*, 2013

They also ranked what they were most worried about from infectious software, as shown in Figure 5.

FIGURE 5

Biggest Fear from Infectious Pirated Software



n = 1,104

Source: IDC's *Dangers of Counterfeit Software Survey*, 2013

These fears are well founded. Using data from the survey and information from other sources, we can quantify the costs to consumers from malware in counterfeit software. These costs include the monetary value of time lost dealing with issues,[10] the cost of paying professionals to help, and the cost to replace lost data or rectify identity theft.

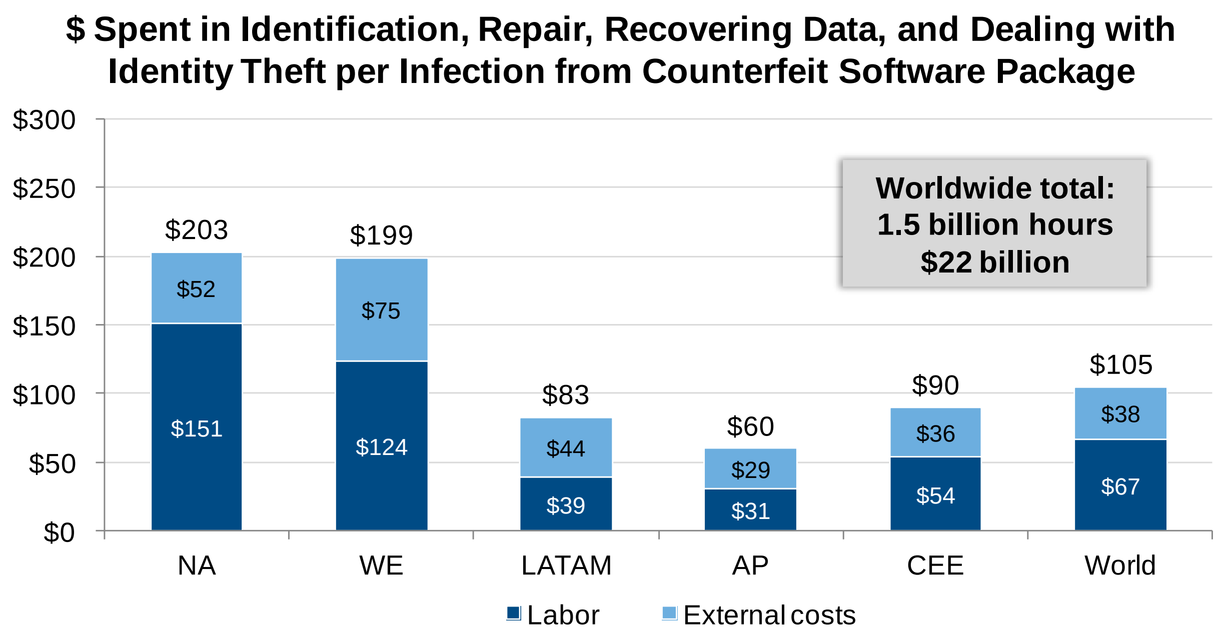
Figure 6 shows the cost breakdown by region per infection related to a piece of pirated software. If you multiply the cost per infection by all the infections from pirated software expected in 2013, you get a total cost of $22 billion and a loss of 1.5 billion hours.

Note that (1) costs per infection are affected by labor rates as well as the percentage of consumers who use outside services to remediate their issues, (2) the world total is closer to the emerging market numbers than those of mature markets because more software (more than 65%) is pirated there, and (3) these figures are averages.

[10] For the sake of quantifying the "hassle" of dealing with security issues, we chose the average hourly wage in a country. Economists will argue that the personal hours lost don't always or even often equate to lost wages, but it seemed a reasonable way to quantify the unasked question of "What would you pay not to deal with this?" The average PC user will also have wages higher than the country average.

FIGURE 6

Consumers' Costs from Infected Software



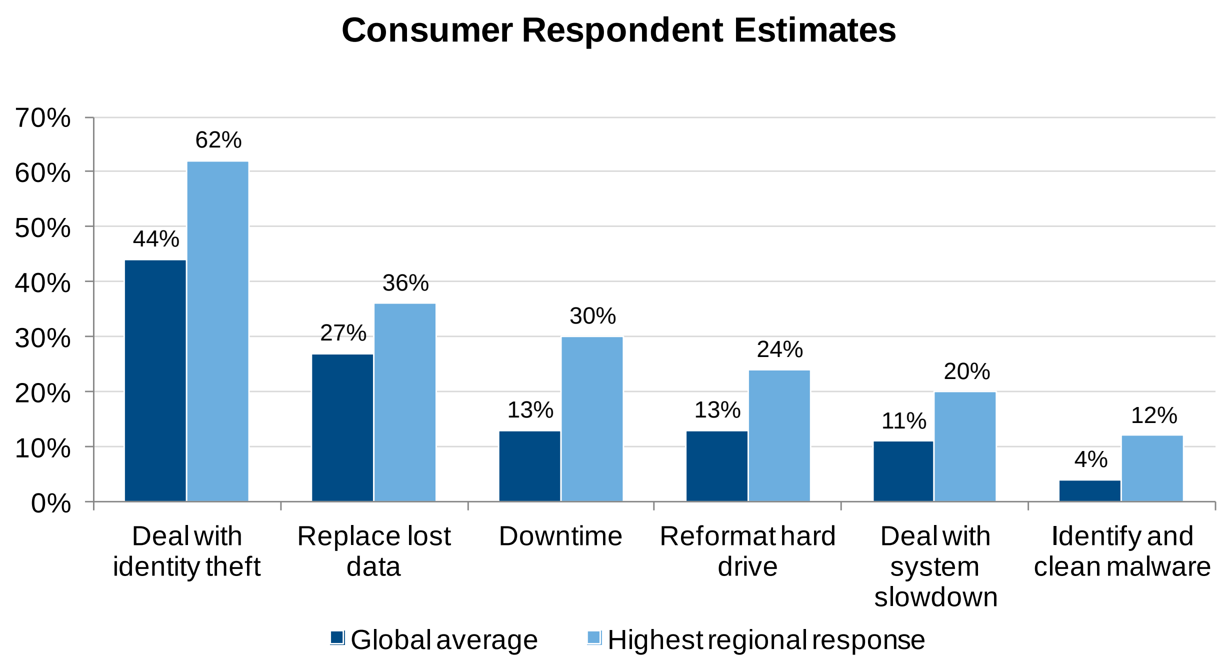
Source: IDC's *Dangers of Counterfeit Software Economic Impact Model*, 2013

The irony is that the best that can happen with an infection from counterfeit software is that existing antimalware programs work and that only some personal time will be lost if other actions need to take place. On the other hand, the *worst* that can happen is a lot worse than the average shown.

For instance, the time to fix problems is calculated based upon the mean of responses from all 10 surveyed countries. However, in some cases, a sizable portion of respondents estimated repair durations more than three to five times the average. See Figure 7, which also shows that estimates differed by geography.

FIGURE 7

Percentage of Problems Requiring More than 10 Hours to Fix



n = 1,104

Source: IDC's *Dangers of Counterfeit Software Survey*, 2013

In addition, the costs to repair can also vary wildly. Professional services for restoring corrupted data files on home PCs can cost as much as $2,500 in the United States.[11] And there are estimates that the 10% of the U.S. households that have experienced identity theft experienced personal losses of greater than $13,000[12] and that the problem required as much as 500 hours over a period of years to clear up.[13]

These costs, by the way, do *not* include the costs of dealing with legal issues, tax audits, penalties, or loss of reputation resulting from being identified by law enforcement as a software pirate.

[11] Author Gantz' personal experience with a crashed disk in 2010.
[12] U.S. Bureau of Justice Statistics press release, November 30, 2011.
[13] "Dealing with ID theft can be expensive, emotionally draining and time-consuming," *Pittsburgh Post-Gazette*, June 9, 2008.

WHAT DOES THIS MEAN FOR ENTERPRISES?

Enterprises have an advantage over consumers — they have professionals focused on protecting their IT assets and budgets for computer security.

But they are not immune from security problems from counterfeit software. IDC has worked with BSA | The Software Alliance to study piracy rates since 2004; this work leads us to believe that enterprises use pirated software less than consumers. Still, we believe that one in three software packages in enterprises is pirated.

Although enterprises have computer security resources that consumers don't have, they are not foolproof.

- In its annual global study of computer security breaches,[14] Verizon found that 69% of "threat events" involved malware, with almost half of that malware on end-user devices. (The study also found that of the breaches caused by agents external to the organization, 83% were attributable to organized criminal groups "deliberately trying to steal information they can turn into cash.")
- In our own survey, 30% of respondents reported security breaches causing network, computer, or Web site outages occurring once a month or more. Of the causes of outages, 50% were from malware on end-user computers.

In other words, end-user PCs are the weak link in most enterprise security defenses.

Now for the bad news.

To begin with, CIO/IT manager respondents told us that 37% of the copies of software they installed or that came with new PCs in the past year had problems: 12% couldn't be installed, 22% couldn't be activated, 20% hadn't been properly licensed, and 11% came with malware.

Workers told us that of the software that IT departments installed on their computers in the past two years, 15% wouldn't run and had to be uninstalled, 19% slowed the computer to where it had to be uninstalled, and 11% infected the PC.

Given worldwide piracy rates, the market for unbranded PCs ("white boxes"), and the percentage of computers shipped with no software on them (28% in our survey), we were not surprised to find in our survey that if the percentage of software coming into the organization was higher in one country than another, so was the percentage having malware. In many cases, it will be the same software.

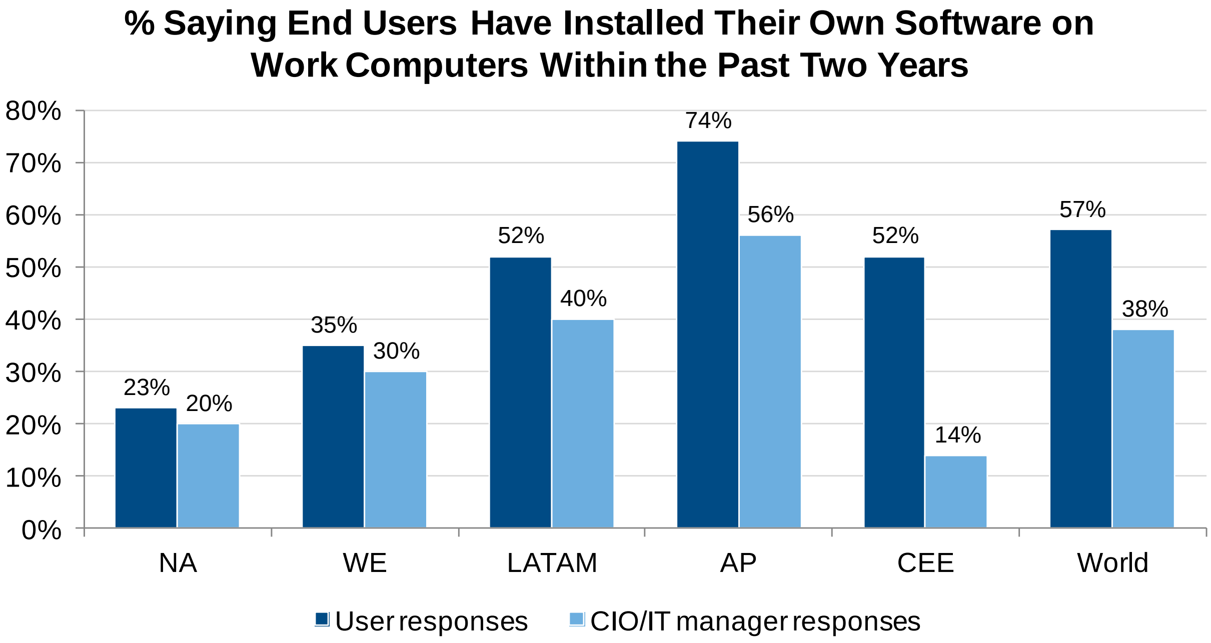
But beyond the treacherous software that comes in the door with enterprise purchases, there is software that end users install themselves on their work computers. Across the full sample, 57% of users said they did so. When we asked IT managers and CIOs the same question, they underestimated how common the practice was, putting the number at 38%.

[14] Verizon's *2012 Data Breach Investigations Report*.

Figure 8 shows the range of responses by region, comparing consumer and CIO/IT manager responses. It seems users are installing more software than their managers think!

FIGURE 8

CIO Blind Spot: End Users Installing Their Own Software



n = 973 business users, 268 CIOs/IT managers

Source: IDC's *Dangers of Counterfeit Software Survey*, 2013

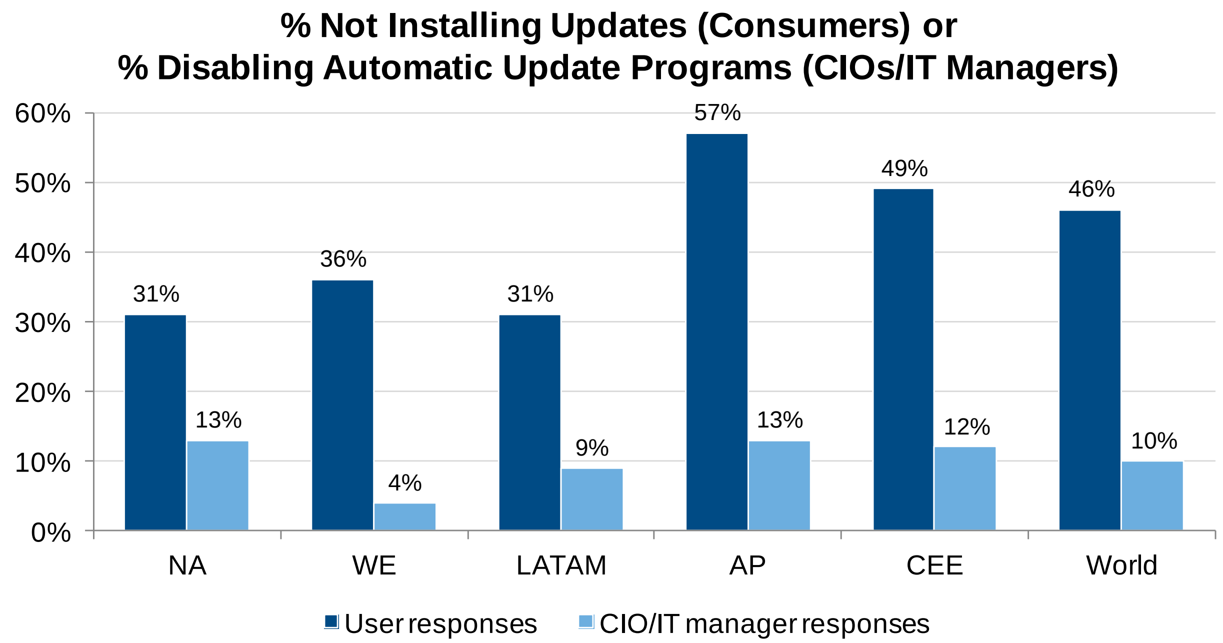
We didn't ask the survey in a way to find out *what* software was being installed — it could be anything from games and home banking software to different versions of commercial software — but we *did* learn that this software is even more problematic than the software installed by enterprises. Business users told us that only 30% of the software they installed on their work computers was problem free, 22% overran their PCs with pop-ups, and 18% worked for a while then stopped. Worse, 21% infected their PC with a virus.

Additionally, 77% of respondents said they use their home computer for work, and 22% said they access enterprise applications and intranets from home using these computers.

But both users and enterprises are not doing themselves any favors in their behavior regarding installing security updates. 46% of consumers told us they don't install security updates, and 10% of IT managers and CIOs told us they have disabled programs that provide automatic updates. Figure 9 shows responses by region.

FIGURE 9

Consumers and Enterprises Not Installing Security Updates



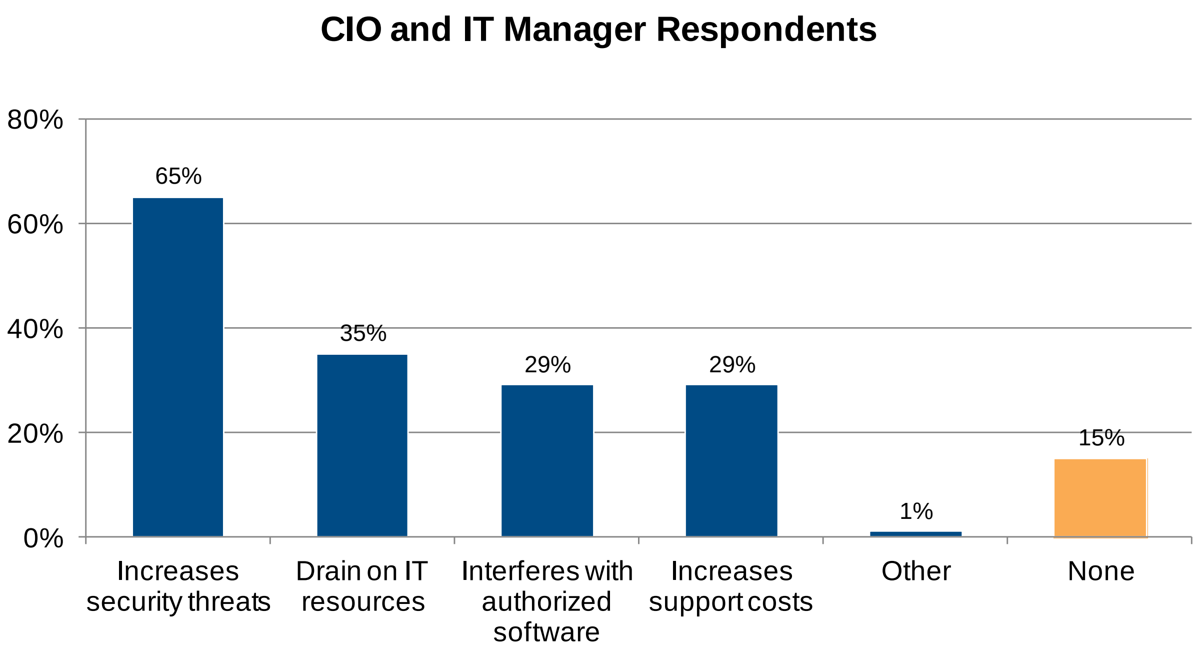
n = 973 business users, 268 CIOs/IT managers

Source: IDC's *Dangers of Counterfeit Software Survey*, 2013

With this level of end-user installation of software on work computers and the potential for malware to be introduced into the organization, you would think enterprises would be assiduous in managing user-installed software. After all, only 15% of IT managers and CIOs told us that user-installed software created *no* problems. The rest had a number of issues, as shown in Figure 10.

FIGURE 10

The Impact of User-Installed Software at Work



n = 268 CIOs/IT managers

Source: IDC's *Dangers of Counterfeit Software Survey*, 2013

At the same time, a full third of IT managers and CIOs didn't audit end-user PCs for user-installed software at all or did so only once a year.

Not coincidentally, those who didn't audit at all reported 34% more security outages resulting from malware on end-user computers than those who *did* audit end-user software.

Finally, as we see in the next section, this user-installed software adds significantly to enterprise cost from malware associated with counterfeit software.

WHAT ARE THE COSTS FOR ENTERPRISES?

Even with less actual counterfeit software in enterprises than on consumer PCs — notwithstanding user-installed software in the workplace — the financial toll for enterprises is greater.

Here are just some of the costs faced by businesses dealing with malware:

- Labor costs of preventing or identifying and rectifying security problems
- Costs of third-party support in dealing with the problems
- Employee downtime
- Costs to locate and reinstall lost data
- Costs of data theft as a result of planted malware
- Costs of fraud from theft of credentials or customer records
- Losses — revenue, time, operational cycles — from Web site, network, and computer outages
- Cost of resources supporting users with stolen credentials

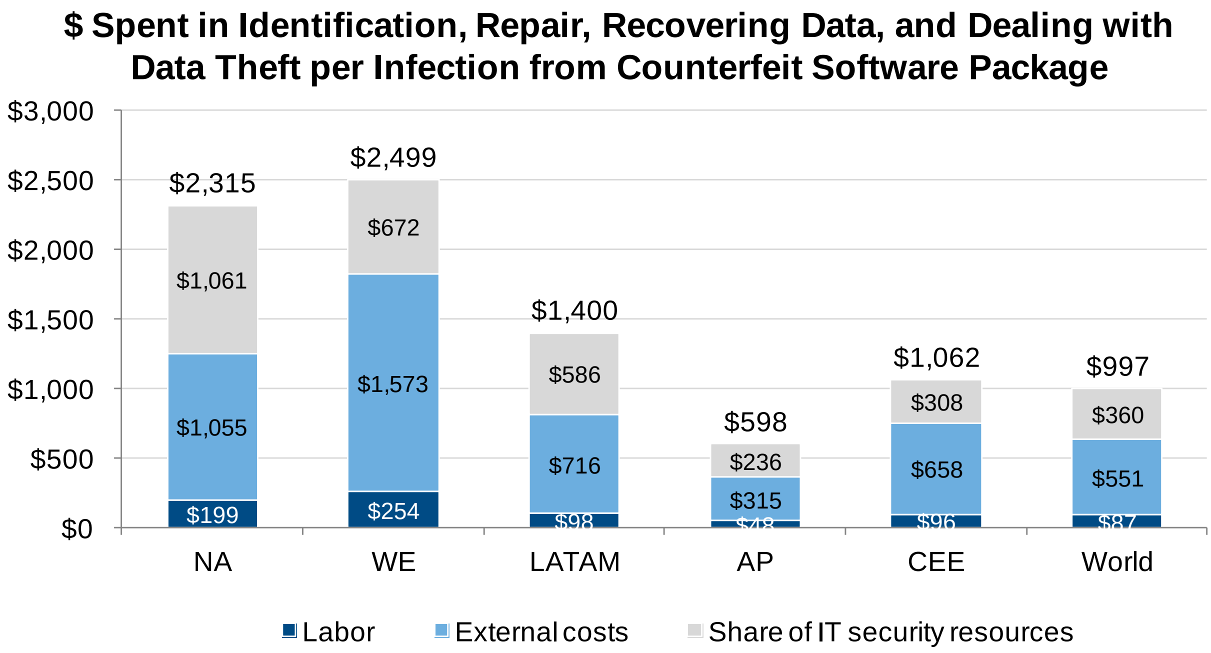
And this doesn't even cover the costs of replacing counterfeit software with legitimate software, going through a software audit, or fines when they are caught with counterfeit software.

What are the actual costs? Using information on piracy rates, IDC information on IT security spending, and information from our survey, we can estimate at least the direct costs to enterprises from malware associated with counterfeit software. That's labor, external spending, and a small share of IT security infrastructure.

Figure 11 illustrates our best estimate of costs per infected counterfeit software program in the enterprise in 2013. Note that the worldwide figure is nearly seven times the costs to consumer per infection. The main reasons for this difference are salary costs for IT professionals that are higher than the wages we used for consumers, cost of employee downtime, higher services costs, and the cost of dedicated IT security resources.

FIGURE 11

The Cost to Enterprises from Infected Software per Incident



Source: IDC's *Dangers of Counterfeit Software Economic Impact Model*, 2013

Add up all these direct costs, and you get expected worldwide losses for enterprises from security issues from counterfeit software of $114 billion. That's equivalent to 8% of IT labor costs.

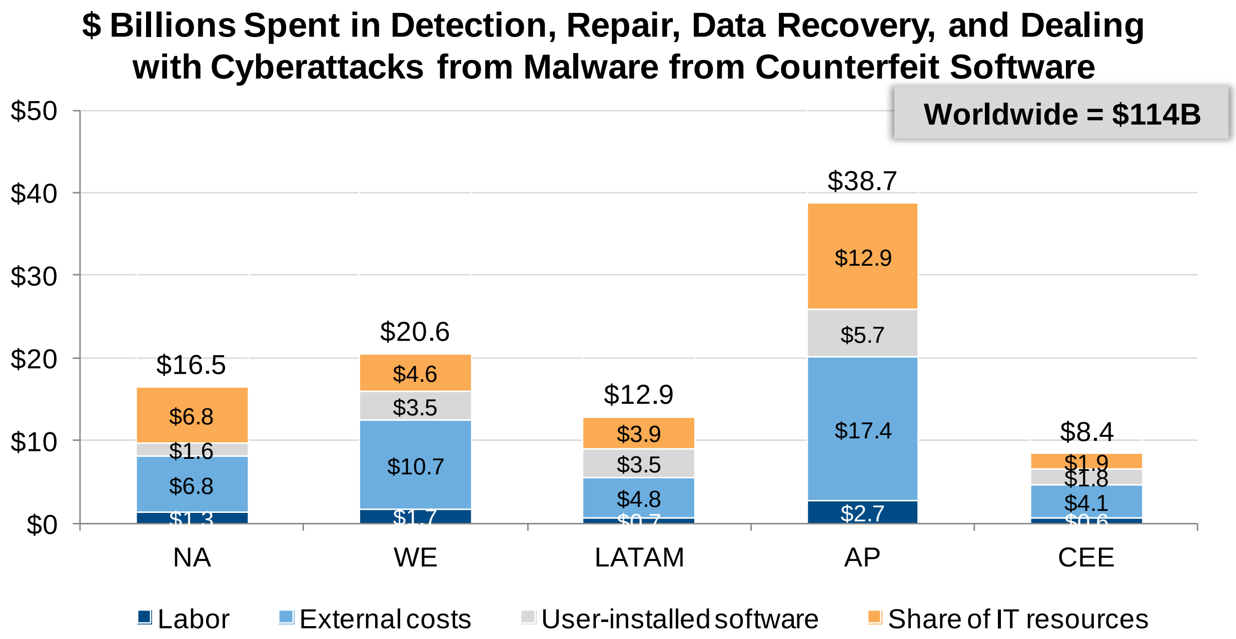
Figure 12 shows that per-unit cost extrapolated across all the infected counterfeit software in enterprises around the world. Note the following:

- The costs are highest in Asia/Pacific despite the fact that labor costs in the region are so much lower than those in the developed world. This is because of the sheer amount of counterfeit units there. Asia/Pacific encompasses 40% of the world's installed base of enterprise PCs and more than 60% of counterfeit software units — not counting those brought to work by end users.

- In fact, the units brought to work — if each user who installs software on his or her work computer installs only one program per year — increase enterprise costs by a third.

FIGURE 12

The Total Cost to Enterprises from Infected Software



Source: IDC's *Dangers of Counterfeit Software Economic Impact Model*, 2013

But enterprises have costs that go well beyond just cleaning and fixing malware on end-user computers. They have the costs of *replicated* security problems — infected computers infecting others — perhaps bringing down the whole network, Web site, or IT system. In fact, in research conducted in China in 2011 for BSA | The Software Alliance,[15] IDC found that pirated software caused systemwide outages or slowdowns nearly once a month for the average size organization. The cost per outage in China was more than $100,000. These costs are *not* factored in to Figure 12.

And problems don't stop at company or even country boundaries. For instance, in our survey, 22% of IT managers and CIOs pointed to malware infections from suppliers or distributors as causing network, Web site, or computer outages. This replication is the reason third-party estimates of the costs of security breaches far exceed our per infected software package values.

For enterprises, the cost of dealing with malware can be even greater. In its 2010 survey of 348 U.S. IT security professionals,[16] The Computer Security Institute found that 50% of respondents had been the subject of a cyberattack, and 67% of those attacks involved malware. And, in the Verizon study mentioned where malware

[15] *Security Risks of Pirated Software: China Businesses Going Legal*, November 2011.
[16] *15th Annual 2010/2011 CSI Computer Crime and Security Survey*, Computer Security Institute.

figured in 69% of data breaches, 61% of data breaches involved a *combination* of malware and hacking.[17]

THE COST OF DATA BREACHES

For enterprises, our threat from counterfeit software story starts simply enough: the prevalence of malware and the costs to deal with it. But the connectedness of enterprise computers and the purpose of some of that malware — information theft, including passwords, account credentials, access codes, etc., — mean that enterprises have exposure far beyond the costs to clean an infected end-user computer.

Take lost information, for instance. In the 855 cases mentioned in the Verizon study cited previously, 174 million records were involved. But what's the value of a record? In the case of TJX, which discovered in 2007 that at least 45.6 million customer credit card records had been stolen by cybercriminals, the ultimate *direct* costs, according to TJX, were $256 million.[18] Third-party estimates were as high as $1.7 billion. This covers the costs of notifying cardholders and giving them advice, legal costs, class action settlements, and internal investigations. So in this case, the cost per record ranged from $5 to $25.

In the Ponemon Institute's *2011 Cost of a Data Breach Study: United States*,[19] the cost per record is $194, but here only large companies (>1,000 employees) and data breaches of 4,500 to 100,000 records are studied, with the average breach about 28,000 records. For data breaches that are the result of malicious attacks, the costs are higher: $222 per leaked record. And to add to our knowledge, 50% of the data breaches from outsiders were from malware.

So, using data from the Ponemon Institute study and our own Dangers of Counterfeit Software Economic Impact Model, we can construct a scenario for these additional costs of data loss. Note that in the Ponemon Institute study, the cost of a data breach is based on what the organization spends to investigate the breach, notify victims, respond to customers and others after the event, and lost business, either from system outages or customer defections.

Figure 13 shows the results of the scenario where one in a thousand infections from counterfeit software results in leaked data. These costs are more than three times the direct costs (although some of the direct costs may be included in the lost data costs), with the global total nearly $350 billion.

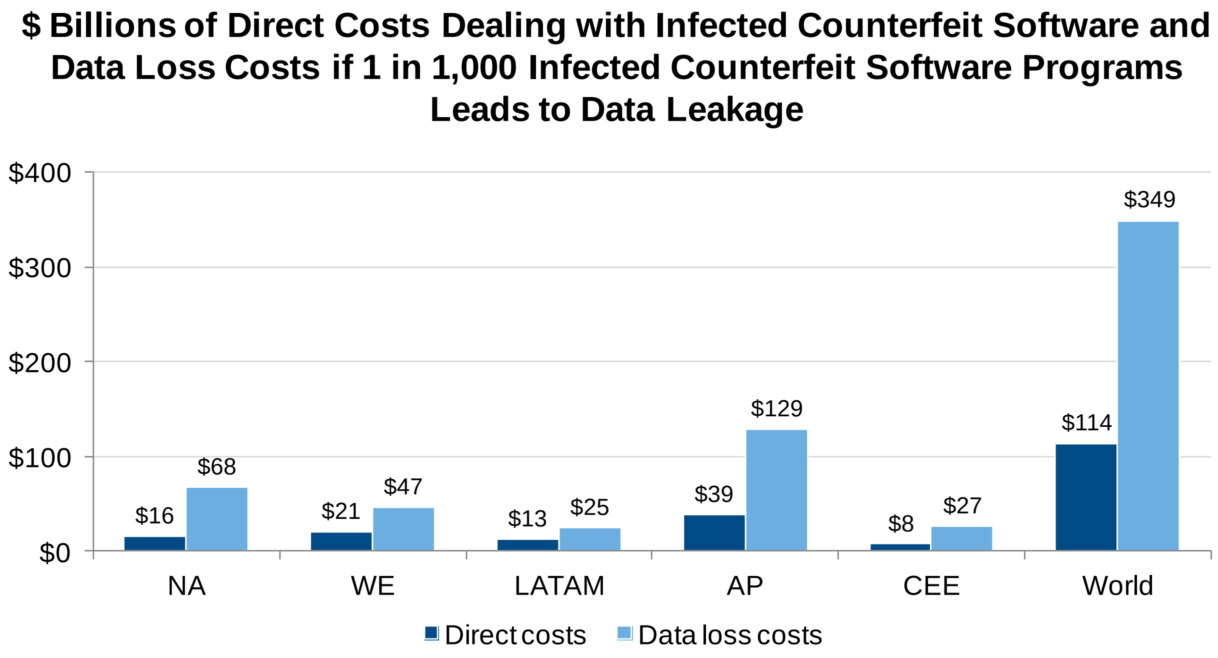
[17] Verizon, op. cit.

[18] "Cost of Data Breach at TJX Soars to $256M," *Boston Globe,* August 15, 2007.

[19] Ponemon Institute's *2011 Cost of Data Breach Study: United States*.

FIGURE 13

Potential Cost to Enterprises from Lost Data



Source: IDC's *Dangers of Counterfeit Software Economic Impact Model*, 2013

Alas, we still haven't plumbed the potential losses to their depths, since the Ponemon Institute study doesn't look at legal costs when customer records result in identity theft, credit card fraud, or illicit access to government or company resources. In the TJX case, the cost of financial reparation was a lot higher than the costs covered in the Ponemon Institute study.

REGIONAL VARIATIONS

We have called out five regions in our economic data and some of the survey data to show the variations in user and enterprise behavior and in financial risks. But the variations extend beyond those charted. Here are some of them:

- **North America.** Despite having the lowest piracy rate of the regions, North America nonetheless has the second highest risk posture because the market is so big: nearly 370 million PCs in place by the end of the year and 45% of the PC software market. Even with a low piracy rate, it accounts for 10–15% of pirated units. Other reasons for its high risk profile are its IT security salaries and its cost per record for data lost, which are higher than those in other regions.

- **Latin America.** Although the region's piracy rate dropped from 66% in 2006 to 61% in 2011, according to the latest published BSA | The Software Alliance study, because of the rapid growth of the region's PC base — by a factor of 2.8 from 2006 to 2013 — and growing user sophistication that leads to more highly configured PCs, the total amount of pirated software has grown by a factor greater than 3.5 from 2006 to 2013. Pirated software is still widely available in street markets — we found it in Peru, Mexico, and Brazil — and selling pirated software is an organized business. Although major urban centers — near universities, Internet cafes, subways — are major sources of pirated software on CD/DVD, it is possible to obtain it in second- and third-tier cities — often copies burned from CDs/DVDs picked up in bigger cities. Prices range from $1.50 in Lima, Peru, to $10 in Sao Paolo, Brazil.

Implications for Nations

The economic impact of malware associated with counterfeit software on consumers and enterprises is covered in depth in this White Paper. But that impact extends to nations as well. Consider the following:

- Governments are enterprises and subject to the same economic impacts as other enterprises. That means at least $10 billion lost worldwide this year to malware associated with counterfeit software.
- The $400+ billion spent on remedial IT work and losses from data breaches is money that could be better spent on more productive activities. If even 1% of that lost money could be spent on IT innovation, based on standard economic ratios, that innovation could lead to $100 billion in new business revenue.
- Given the global and complex nature of industrial supply chains, malware that originates with counterfeit software in one country can easily endanger computers in another. Dealing with this soaks up resources better used to support the local economy.
- Malware, whether imported or from domestic sources, leads to a less secure national infrastructure and enhanced vulnerability to cyberattacks.

- **Western Europe.** Counterfeit software is almost entirely either found on the Internet or copied from one user to another. Even in 2006 we were unable to find software for sale in any kind of street market. It *is* possible, however, to find it on PCs and software moving through the channel: 14% of consumers we surveyed in Western Europe said they found some pirated software installed on new computers they bought. The same percentage of CIOs/IT managers we surveyed said the Microsoft Office that came preinstalled with new PCs was improperly licensed. But they also said nearly 10% of the PCs they installed in the past two years were self-built or self-assembled and that 34% of the PCs they purchased came with no operating system. As for the region's risk profile, the PC installed base in Western Europe is 10% smaller than that of North America, and IT staff spending is a third less. So Western Europe's financial risk from malware in counterfeit software is a third less. Its exposure to lost data is almost half that of North America because of fewer records lost per breach and a lower loss per record.

- **Central and Eastern Europe.** Although classified as an emerging market, the region has some characteristics of developed markets, such as fairly high education levels and some top-notch programmers — as well as top-notch hackers and virus creators. According to an interview published in the German newspaper *Der Spiegel* in 2011,[20] Russia lags only China and Latin America in the production of malware. Users in Russia, however, have the same behavior and attitudes as users in the other regions in our surveys. They make fewer PCs from scratch than Western Europeans, and they have less frequent security outages. But the region *does* account for about 10% of pirated software in the world. It is getting harder and harder to find counterfeit software in the region in CD/DVD format, but Internet access has grown to where nearly half the population uses it, and 25% of households have broadband access.

- **Asia/Pacific.** This is the largest region in the study in almost all respects. It contains more than half the world's population, nearly half the world's Internet users, and 40% of the world's PCs — not to mention half the world's pirated software. Our enterprise survey respondents told us that 32% of their PCs come without operating systems, and 13% don't install security updates. 57% of consumer respondents don't install security updates, and nearly 70% of consumers who use pirated software have had problems with it. On the ground, we found no problem acquiring CD/DVD versions of software in street markets, although in China, there seems to be a greater likelihood of getting a CD/DVD burned at the point of sale than prepackaged. The Web sites offering counterfeit software appeared to be supported by advertising revenue rather than clandestine sites seeking to extract personal data. But then, it was a small, Beijing-oriented sample. Prices varied, but around $4–7 for CDs/DVDs that contained copies not only of Microsoft Office but also of malware was the norm. The region's economic risk is high — because of the sheer amount of counterfeit software and the infection rate — but it is ameliorated by comparatively low wages and smaller and less costly data breaches.

FUTURE OUTLOOK AND CALL TO ACTION

Since we conducted our first study on the dangers of counterfeit software in 2006, piracy rates dropped in a majority of countries — but the global piracy rate went up because the market for PCs shifted to emerging markets with higher piracy rates, the amount of counterfeit software increased, and the creation and deployment of malware became a bigger business. The counterfeit software environment may be slightly less infectious, but not by much.

[20] "Anti-Virus Pioneer Evgeny Kaspersky: I Fear the Net Will Soon Become a War Zone," *Der Spiegel*, June 27, 2011.

Yes, over the next seven years, the installed base of PCs will grow by a factor of less than 1.5 — versus a factor of 3 in the past seven years — but software-laden phones and tablets will take up the slack. And these mobile devices may be even harder to manage — and keep secure — in enterprise settings than PCs.

Nor is it likely that the creators of malware and of counterfeit software will depart a lucrative business that may be one of the safest criminal environments within which to operate.

It seems logical to infer, then, that the security risks faced by users of counterfeit software can only increase. Which is the reason we conducted this research: to quantify those risks and help end users and enterprises become aware of them.

There are ways to prevent attacks like those we detected, such as installing firewalls on your PC, being attentive to security updates, monitoring end-user installation software in the enterprise, using up-to-date antimalware tools, and adhering to good security practices and policies. New techniques like application whitelisting, where only trusted programs are permitted on a computer, and better browser security can also help.

But the best prevention is simply to use the genuine item. This means procuring computers and software from trusted sources, avoiding software with too-good-to-be-true prices, and following activation and registration protocols.

APPENDIX

Methodology

Lab Tests

To assess the risks of obtaining and using pirated software and activation tools, IDC set up testing labs within its own IT departments in Framingham, Massachusetts; Prague; and Beijing. Using normal search techniques on popular search engines, each lab developed a list of Web sites/P2P networks for pirated software and then navigated those sites and downloaded software from them. We also tested sites that offered key generators and other activation bypass tools, since those are so often required even after a program is installed. After a while, we would turn on our antimalware and spyware removal tools and record results.

We also attempted to install some of the copies of Microsoft Office we downloaded and ran malware tests on those we could install to discover additional malware and quantify the need for additional activation bypass tools.

Finally, we obtained CD/DVD versions of Microsoft Office from street markets in Brazil, China, India, Mexico, Peru, and Thailand and tested them in a manner similar to the downloaded software.

Our tests were conducted in January 2013 by individuals working at virtual machines running the latest versions of commercially available antivirus and spyware removal software in the tests. All our machines had the latest security updates. After each test, we reinstalled the virtual PC to make sure the next test wouldn't be contaminated by malware from a previous test.

Table 1 shows the extent of our testing.

TABLE 1

Test Results

Web sites/P2P networks searched	270
Software downloads	108
CD/DVD program tests	155
Total	533

Source: IDC's *Dangers of Counterfeit Software Survey*, 2013

Three points:

- We believe that our search protocol and the sheer number of sites we tested meant that we tested a significant sample of the most popular download sites.
- We chose to concentrate on Microsoft Office because it is installed on a majority of PCs and it is one of the most pirated software programs on earth.
- We also believe that malware creators will target Microsoft Windows more than Microsoft Office, and other software types less than Office, thus making Office a good proxy for all counterfeit software.

Surveys

During January 2013, IDC conducted two global surveys: one of consumers and workers and one of CIOs/IT managers. The surveys extended across 10 countries: Brazil, China, Germany, India, Mexico, Poland, Russia, Thailand, the United Kingdom, and the United States. The total sample included 1,104 consumer respondents, 973 business user respondents, and 268 CIO/IT manager respondents.

In the CIO/IT manager sample, 47% of respondents came from organizations with more than 1,000 employees and 53% came from smaller organizations. In the survey of workers, 40% worked at organizations with more than 1,000 employees, 18% at organizations with fewer than 100 employees, and 42% at organizations with between 100 and 1,000 employees. The industry mix in both surveys was representative of the general economies.

The surveys were conducted via Internet using third-party panels of computer users and CIOs/IT managers and asked questions about PC and software purchases, end-user installation of software in enterprises, issues around problem software, and attitudes and behavior toward security problems. They also asked respondents to quantify the time spent dealing with security issues, which were used as inputs for the economic impact data presented in this White Paper.

Note that in figures referring to survey data where we break out regions, the label "World" means the unweighted total of all respondents.

Note: All numbers in this document may not be exact due to rounding.

Economic Impact Modeling

To develop the economic impact figures in this White Paper, we developed a Dangers of Counterfeit Software Economic Impact Model that incorporated proprietary data from the IDC BSA | The Software Alliance 2012 Global PC Piracy Study, survey results from the survey conducted for this project, IDC IT spending and PC research, and third-party data referenced in the figures.

Two key starting points were:

- The chance of infection by region
- The total number of counterfeit software units by region

In both cases, regions were developed using a 20-country superset of the 10 surveyed countries for which we had BSA study data. These 20 countries account for more than 75% of pirated software in the world. We developed rest-of-region estimates to complete the global picture.

We developed the "chance of infection" estimates using data from our lab tests with allocations by source of the software — from street markets, from the channel, from the Web, etc. Using data from the BSA work, we developed counts by region for pirated software units (estimated for 2013 based on the 2011 study), which we factored down to get to *counterfeit* units. The factoring relied on BSA data on the source of pirated software and other proprietary work IDC has done in the past (e.g., percentage of pirated software resulting from misuse of volume licensing).

This done, we had a picture of the number of counterfeit units of software for 2013 and what percentage would be infected. The next step was to estimate what percentage of the infections would be routinely caught by user and enterprise antimalware software without requiring any further action. Here we used the percentage that chose not to install security updates as our proxy figure.

After that, we took survey data on the time to fix various security issues and applied it to the number of counterfeit infections per region to come up with time spent per infection. This led to the total hours spent by region dealing with infections from counterfeit software.

We then used data available from the U.S. Bureau of Labor Statistics on IT salaries and third-party data on average wages per country to extrapolate the direct labor hours fixing security issues for both users and IT organizations. Using IDC data on the size of the third-party security industry, we were able to estimate the percentage of the time outside resources had to be used and, again, the cost per infection. Finally, we used that same data to develop the share of IT resources devoted to IT security (networks, firewalls, antimalware software, etc.) that would apply to malware from counterfeit software.

Altogether, this data yielded the per-infection and aggregate regional costs to deal with security issues resulting from counterfeit software.

The data breach information was developed using estimates from the Ponemon Institute on data loss costs per data record leaked and average number of data records compromised per breach for a handful of countries.

Note: All numbers in this document may not be exact due to rounding.

Copyright Notice