WHITE PAPER

The Link between Pirated Software and Cybersecurity Breaches

How Malware in Pirated Software Is Costing the World Billions

Sponsored by: Microsoft

IDC

John F. Gantz
Alejandro Florean
Richard Lee
Victor Lim

NUS

Biplab Sikdar
Sravana Kumar Sristi Lakshmi
Logesh Madhavan
Mangalam Nagappan

March 2014

A Joint Study by National University of Singapore and IDC

IN THIS WHITE PAPER

This White Paper presents the results of joint research by National University of Singapore and IDC of the prevalence of malicious code (malware) found in pirated software and in PCs purchased through distribution channels. It also looks at the link between the detected malware and criminal organizations, for which malware in pirated software can be a lucrative vector for cyberattacks.

This study provides an economic analysis of the costs associated with malware on pirated software. It is supported by forensic analysis conducted by National University of Singapore on 203 computers acquired in 11 countries: Brazil, China, India, Indonesia, Mexico, Russia, South Korea, Thailand, Turkey, Ukraine, and the United States. It is supported by a survey of 951 consumers and workers, and 450 CIOs/IT professionals from 15 countries: Brazil, China, India, Indonesia, France, Germany, Japan, Mexico, Poland, Russia, Singapore, Thailand, Ukraine, United Kingdom, and the United States. It also contains results from a survey of 302 government officials from six countries: Brazil, China, India, Mexico, Russia, and Singapore.

EXECUTIVE SUMMARY: CRIMINALS COULD STEAL BILLIONS

One of the hidden costs of using pirated software is the likelihood of encountering nasty, unwanted code, either in the software itself, via code that can get downloaded or installed along with it, or on PCs with pirated software installed on them. Much of this malware is created by criminal organizations with illegal financial gain, data theft, espionage, or other mayhem in mind.

IDC research shows that:

- Consumers and enterprises have a 33% chance of encountering malware when they obtain and install a pirated software package or buy a PC with pirated software on it.
- The National University of Singapore forensic analysis of 203 PCs purchased in 11 countries with pirated software on them found 61% of those PCs infected with malware.
- Consumers will spend nearly $25 billion and waste 1.2 billion hours in 2014 dealing with security issues created by malware on pirated software.
- When asked about their biggest fears associated with a security event, 60% of consumers put loss of data or personal information in the top three, and 51% placed unauthorized access or online fraud in the top three.
- Despite these fears, 43% of consumers don't routinely install security updates on their computers.
- The biggest fears of government officials polled were loss of business trade secrets or confidential data (cited by 59% of respondents), unwanted access to government information (cited by 55%), and cyberattacks on critical infrastructure (also cited by 55%).
- In 2014, IDC estimates that enterprises will spend $491 billion because of malware associated with pirated software, which breaks out to $127 billion in dealing with security issues and $364 billion dealing with data breaches.
- Almost two-thirds of these enterprise losses, or $315 billion, will be the result of the activity of criminal organizations.
- Because of its large installed base of PCs and high piracy rate, the Asia Pacific region will incur more than 40% of worldwide consumer losses and more than 45% of enterprise losses from malware on pirated software.

WELCOME TO THE WORLD OF MALWARE

Just as humans can be infected by microbes like those "wee beasties" first observed by Anton Von Leeuwenhoek back in the 1600s, computer software can be infected by digital microbes, which as a group are called malware. Their names alone evoke danger: Trojan horse, virus, keystroke logger, password stealer, backdoor, spyware, ransomware, netbot. These are the pathogens of the digital world.

But if they are not borne of nature, where do they come from?

Actually, there is a whole industry that creates and distributes them, as described in this year's Annual Security Report by Cisco Systems.[1] At the top of the malware business pyramid are the hackers who create new tools and discover new vulnerabilities. In the middle are those who offer services, like hosting the servers to send out malicious spam, or who offer exchanges for buying and selling malware and malware tools. At the bottom are the miscreants themselves, the users who want to make money from the malware or activists who want to make a point.

[1] www.cisco.com/en/US/prod/vpndevc/annual_security_report.html

Case in point: SpyEye is a tool kit created in 2010 by a Russian hacker named Sasha Panin that used tools like data grabbers and keystroke loggers to collect personal and financial information. Prices for SpyEye, sold on a Web site called darkcode, ranged from $1,000 to $8,500. SpyEye could fake bank Web sites and grab customer credentials and account data and could steal credit card data off infected computers. By the time Panin was apprehended in 2013, SpyEye had infected 1.4 million computers.[2]

The malware market is an active one – one that reacts to supply and demand. For instance, according to an article last year in CSO Magazine's online edition[3] entitled *Prices Fall, Services Rise in the Malware-as-a-Service Market,* competition drove the cost of a botnet comprised of 1,000 infected computers in the United States from $200 to $120 in just two months.

This article also points out the growth in malware-as-a-service sites, where users pay $100-$200 a month to third parties to host their malware tools. There are also sites that rent access to networks of computers pre-infected with malware.

The malware-producing industry is, in fact, sophisticated enough now that there are even Web sites offering standardized services to help malware tool and service creators set up shopping sites for customers, as described in the Webroot Threat Blog.[4]

How big is this malware market?

No one has taken a stab at sizing it, but a reasonable proxy could be the stolen credit card market, since one of the goals of malware is to obtain personal information. If stolen credit card data can be sold for as much as $100 a card, and if a billion such records were stolen in 2013,[5] then simple math would indicate that the malware market could easily be $50 billion[6] this year.

So, malware that infects your computer most likely came from some criminal enterprise in search of financial gain. And one common way malware gets to *your* computer is via pirated software.[7]

---

[2] See the story in USA today, published March 5, 2014, "Meet the Architects of Data Theft: How the Feds Tracked Down a Notorious Russian Hacker." http://www.usatoday.com/story/news/2014/03/05/hackers-prowl-dark-web/5982023/

[3] www.csoonline.com/article/729655/prices-fall-services-rise-in-malware-as-a-service-market

[4] From the Webroot Threat Blog, *Newly launched managed 'compromised/hacked accounts E-shop hosting as service' standardizes the monetization process*, www.webroot.com/blog/2014/01/24/newly-launched-managed-compromisedhacked-accounts-e-shop-hosting-service-standardizes-monetization-process/

[5] www.usatoday.com/story/cybertruth/2014/01/28/cybercrooks-use-stolen-consumer-data-hour-to-hour/4968887/

[6] Not all credit card theft is related to malware – some may be the result of physical theft or physical devices that record data from card readers, but then again, credit card information is not the only cybercriminals obtain. But let's say with all that put together the market for the information gained from malware *is* $100 billion. A normal business chain model would indicate that between 20%-80% of that could pay for the tools and infrastructure to generate the revenue.

[7] What is the difference between pirated and counterfeit software? All counterfeit software is pirated, but some pirated software is legitimate software that is under-licensed. In all calculations in the White Paper where we say pirated software, we assume that pirated software that is not counterfeit is uninfected.

THE INFECTION RATE OF PIRATED SOFTWARE

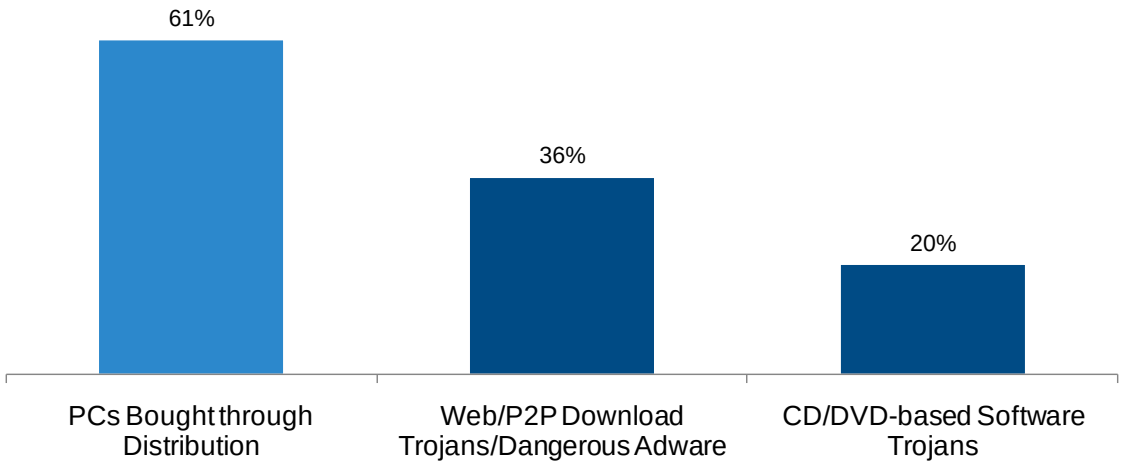
In 2013[8] IDC tested pirated software from more than 550 Web and P2P sites or CDs bought in street markets to determine the prevalence of malware in pirated software. In January and February of 2014, the Department of Electrical and Computer Engineering at National University of Singapore conducted a forensic analysis of 203 PCs that were purchased from PC resellers, specialty shops, and PC markets in typical buying situations in 11 countries. Together, this research found the chances of encountering malware in a pirated copy of software is one in three. The chance of encountering malware in a PC purchased with pirated software is more than 60%.

Some of this malware may be cleaned or blocked by antimalware programs, but certainly not all of it. There are a number of reasons: infections in base software, as they are in operating systems, may be hard to detect; some pirated software disables functions that make it easier for PCs to get infected by malware from elsewhere; and many users, especially those deliberately using pirated software, don't install security updates. The NUS team actually used five different anti-malware programs in order to find all the threats and each time a new program was used more threats were found. Many PC users will have only one such program.

Figure 1 shows the infection rates of pirated software by source of infection.

FIGURE 1

Infection Rates by Source



Source: IDC 2013 lab tests and National University of Singapore forensic analysis, 2014

[8]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. March 2013, www.microsoft.com/en-us/news/download/presskits/antipiracy/docs/idc030513.pdf

GETTING A NEW PC? BUYER BEWARE

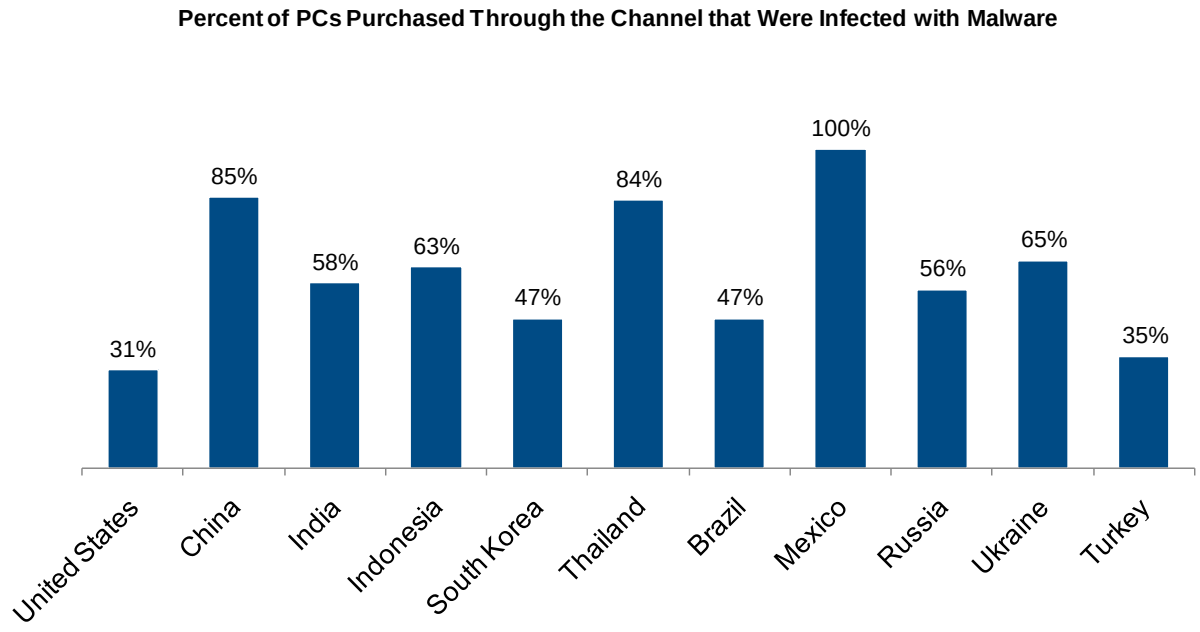
This National University of Singapore research on malware on PCs purchased from common distribution sources – computer specialty shops, resellers, and local markets – found that 46% of the PCs came with dangerous malware.

The malware included viruses, worms, Trojan horses, rootkits, and unwanted Adware, which had pre-infected the new PCs before they could even access the Internet. There were other problems as well, such as misleading applications, corrupted executables, exploits, and system vulnerabilities, which we didn't count as "infections" but that can contribute to the problem. Exploits, for instance, are often used to allow the pirated software to function. But these vulnerabilities can make it easier for the PCs to get infected once they *do* have access to the Internet.[9]

Figure 2 shows the summary results by country studied by the National University of Singapore. Note that in the forensic work, more than 100 discrete threats were discovered, making an average of 3.0 per PC. And a single threat could infect multiple files.

FIGURE 2

Infections with New PCs



Source: National University of Singapore forensic analysis, 2014

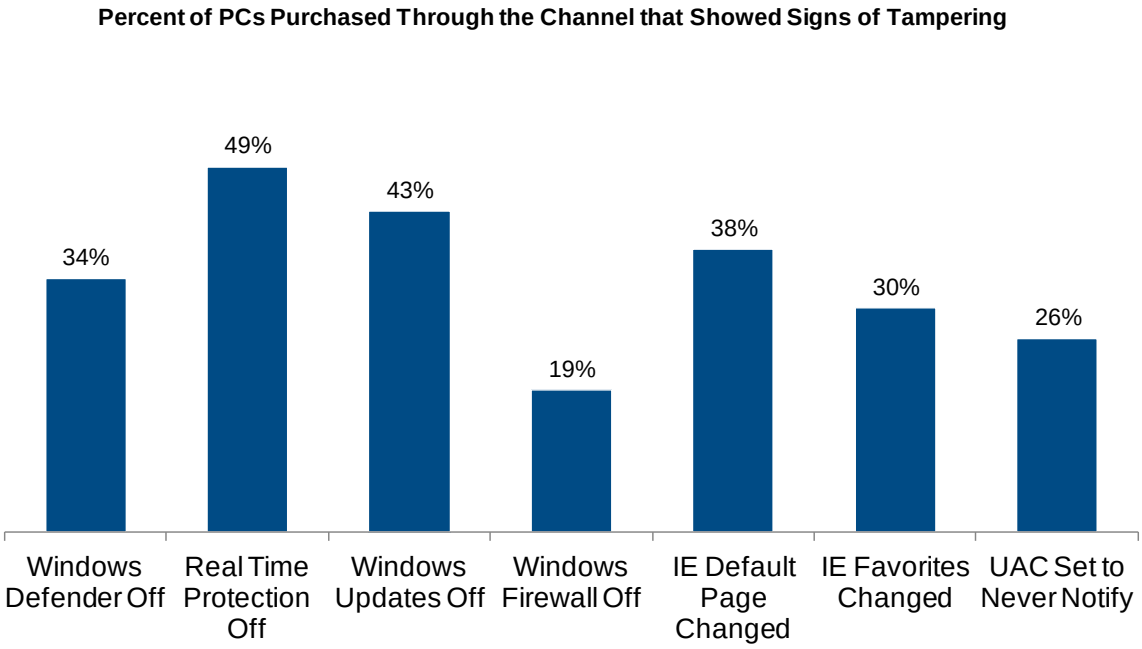
[9] A full list of malware definitions can be found in the Microsoft Malware Protection Center at www.microsoft.com/security/portal/mmpc/shared/glossary.aspx

But malware isn't all you find on pirated software bundled with PCs. The National University of Singapore team also found a high rate of tampering has taken place on the software. Figure 3 shows different forms of tampering by type, ranging from security features that were disabled to browser default settings that were changed and the notification service that tells you when applications are trying to make changes to your PC.

Figure 3 shows you the high level of tampering.

FIGURE 3

Tampering Analysis of PCs with Pirated Software Bought via the Channel



Source: National University of Singapore forensic analysis, 2014

How do you avoid the unwanted and potentially infected software that comes with your computer?

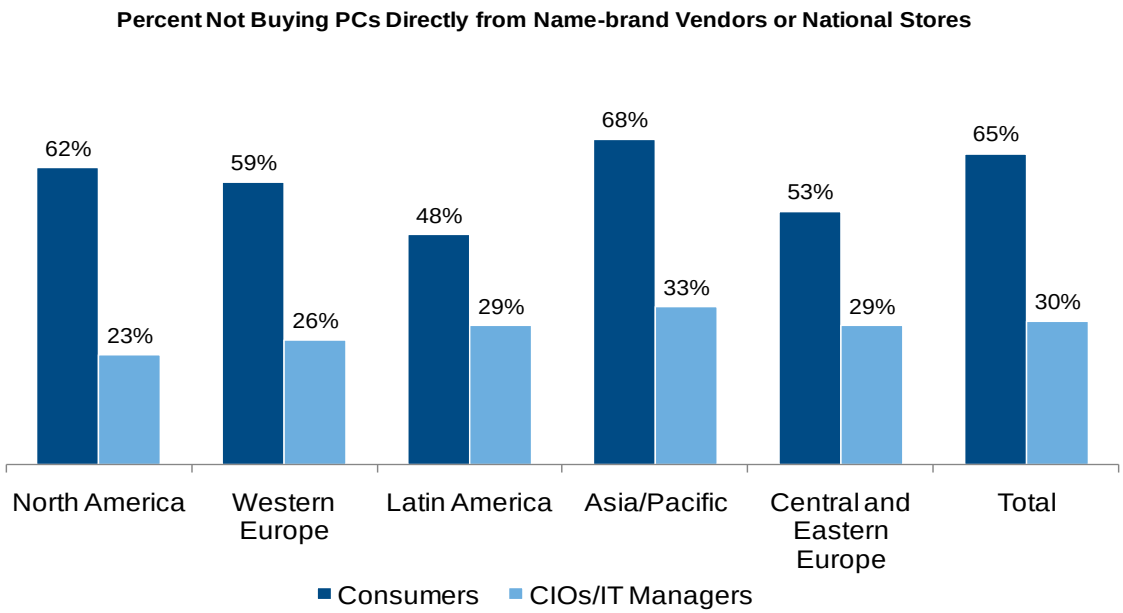
Probably the best way is to buy only from name brand computer vendors or a national retail chain. But in our survey, 30% of enterprise respondents bought from other, more suspect sources, as did 65% of consumers.

These sources included computer specialty shops, consultants, non-branded PC assemblers, online stores/trading portals, auction sites, flea markets, and yard sales. They also include PCs received as gifts and self-built PCs.

Figure 4 shows survey results for both communities.

FIGURE 4

PCs from Suspect Sources



n = 951 consumers, 450 CIOs/IT managers

Source: IDC, 2014

Not all of these suspect sources will automatically install pirated software on PCs – for example online stores may not – but, then again, there may be some pirated software even on PCs that come from more trusted sources. The best way to buy a PC without malware is to buy from a trusted source – and then install security software on it and update and run it regularly.

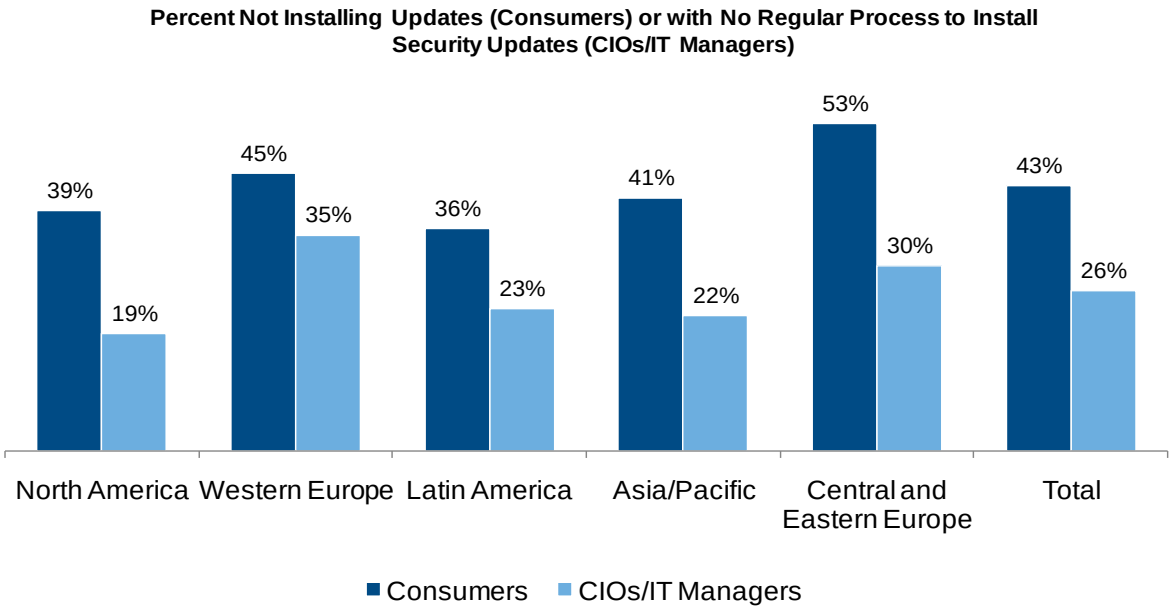
HOW DANGEROUS IS THIS MALWARE?

Some of the exploits and Trojans National University of Singapore found seemed innocuous enough, as they targeted vulnerabilities that have been addressed by published security updates.

Alas, in our survey we found that many people and enterprises don't regularly install their security updates, as shown in Figure 5.

FIGURE 5

Inattention to Security Updates



n = 951 consumers, 450 CIOs/IT managers

Source: IDC, 2014

In fact, Microsoft and others have found that even the dreaded "zero day exploit," in which malware creators found and exploited vulnerabilities before the vendor could get a security patch out, were not that critical. In the Microsoft analysis, less than 0.2% of the problems users found using Microsoft security tools in a year were related to such fast-turnaround malware.[10]

And National University of Singapore found more than 100 distinct threats, some of which were quite nasty. Here are just three of them.

- **Win32/Enosch.A.** This is a worm that searches for all Microsoft Word documents (.doc and .docx) in the infected computer and emails them to a remote attacker.
- **Win32/Sality.AT.** This is a virus that stops some security software and some Windows utilities from running. It also tries to download other files from a remote server, including other malware.
- **Win32/Pramro.F.** This is a Trojan that creates a proxy server on an infected computer. The proxy server may then be used to relay spam e-mail and web traffic as well as to hide the origin of the attackers responsible to the malicious activity.

In short, the malware you might find on your pirated software could:

- Steal your passwords
- Imitate your banking site
- Log your keystrokes
- Redirect Internet search results to dangerous sites
- Gather your contact information and send fake emails from your computer
- Use your computer as part of a denial of service attack
- Identify and steal confidential or secret information
- Allow hackers free access to your system

It could even take control of your computer. In the 2013 IDC research, analysts actually found malware taking control of the camera on the PC and recording them.

[10] See Microsoft Security Intelligence Report, Volume 11 www.microsoft.com/security/sir/archive/

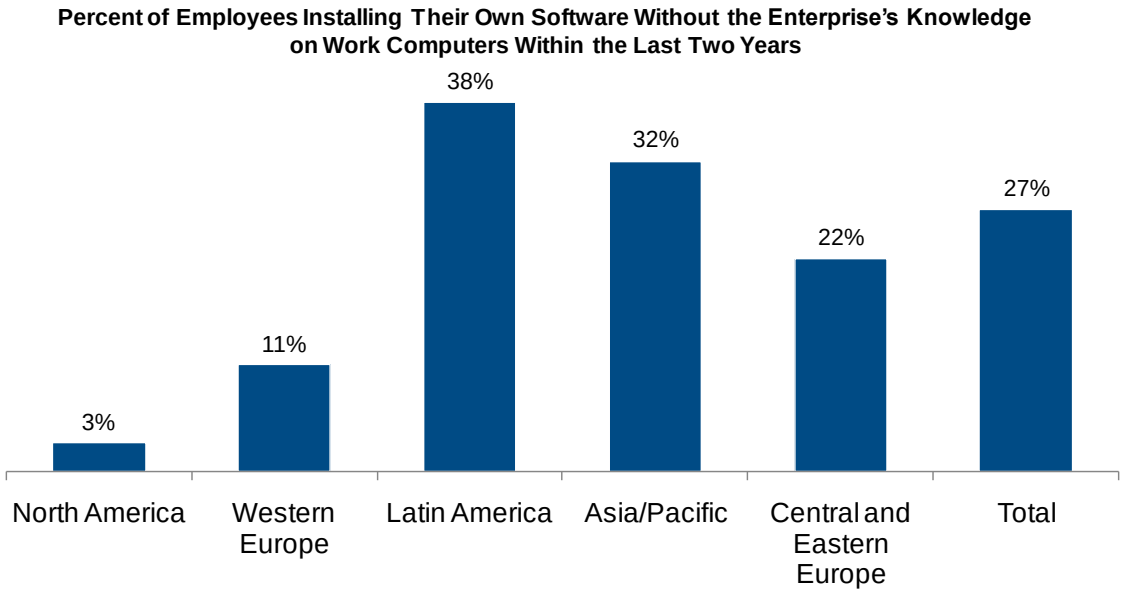
THE IMPACT OF END USERS ON THE ENTERPRISE

IDC believes that, in general, consumers use more pirated software than enterprises. And a surprisingly large percentage of employees bring their own software, which is often pirated, to work. It can be installed on a laptop taken home, downloaded from the Internet, or even installed at work from borrowed or personal copies of pirated software.

In this year's survey we probed this topic, asking how often employees installed software on their work computers without their organizations' knowledge. Twenty-seven percent of respondents said they did. Based on the number of programs they installed, IDC estimates that nearly 20% of pirated software in enterprises is put there by employees. Figure 6 shows the breakdown by region.

FIGURE 6

BYO Pirated Software



n = 951 consumers/employees

Source: IDC, 2014

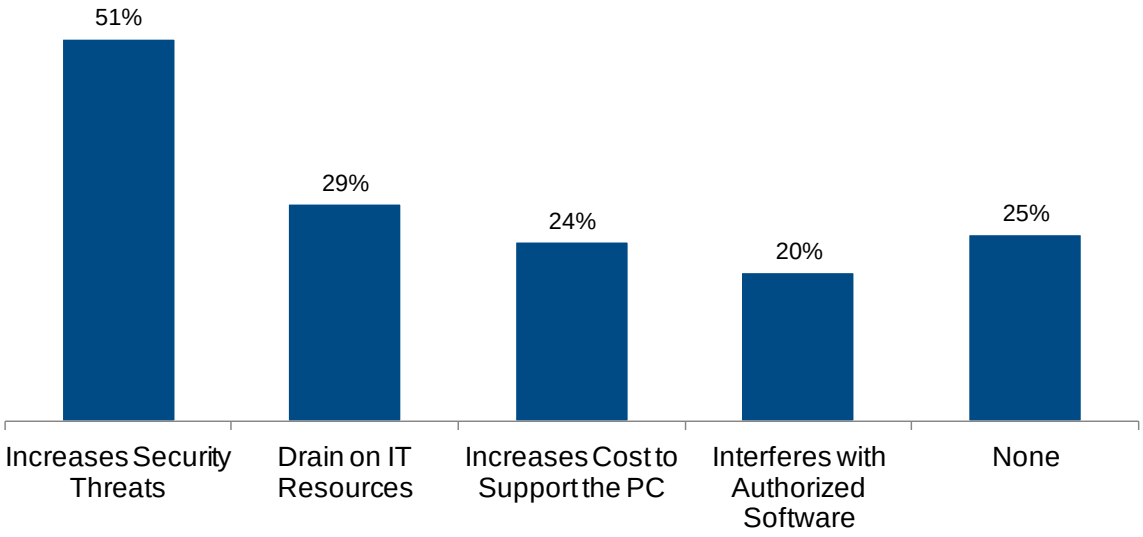
While the differences by region look a little lopsided, the difference in the average number of software packages installed per user doing so was much tighter from region to region, ranging from 3.3 to 4 a year.

When we asked CIOs about employee-installed software, they seemed well aware that the practice was going on and had a reasonable understanding of the extent; 75% felt that it created problems for them.

Figure 7 shows the problems they foresaw, with security being number one.

FIGURE 7

Problems with Employee-installed Software at Work



n = 450 CIOs/IT managers

Note: multiple responses allowed

Source: IDC, 2014

And while 71% of CIOs and IT managers responding said their organizations had programs to audit software on end-user computers, 39% of them conducted such audits less than once a year. In other words, more than half of end-user PCs have no effective audit.

THE REINFECTION QUESTION

A key question of concern to business and consumer users alike is whether infected computers will infect others. In our survey, CIOs and IT managers indicated that 30% of their system, network or Web site outages were involved in malware infections from suppliers or distributors; 15% of consumers worried about infecting others with any malware they may have on their computers.

Not all malware propagates itself. For example Trojans, which accounted for more than 40% of the threats discovered by National University of Singapore, do not. But Trojans can still be used to launch other attacks. There is even a term called "pivoting," which refers to the introduction of malware onto a system in one place that is then used to launch a more sophisticated attack on a bigger target.

This theme is echoed in the Cisco 2014 Annual Threat Report, which states that, "the end goal of many cybercrime campaigns is to reach the data center and exfiltrate valuable data. A malicious action occurs on a device outside the corporate network, which causes an infection, which moves to the network, and then to the treasure trove: the data center."[11]

And last year we saw an example of an extreme form of re-infection: the Citadel botnet, which created 5 million zombie computers across 90 countries that recorded keystrokes and could then capture login passwords and other personal information and records. The zombie computers sent this information back to criminal organizations in Eastern Europe, which eventually stole half a billion dollars from consumers and enterprises.[12] Citadel was created on a well-known Trojan, "Zeus," and its source code, which was also a notorious financial bot which engaged in wire fraud, bank fraud, and access device fraud. These two malicious financial botnets were finally taken down by Microsoft, other industry partners, and law enforcement in 2013. Court records show that the cybercriminals behind the Citadel botnets infected PCs in part by selling pirated versions of the Windows pre-infected with the malware.

The National University of Singapore forensics also found that one virus, worm, or Trojan could infect more than one software program and could be lodged in multiple directories on a PC. In one PC sample from India, the team found 1,000 infections, including 788 from one virus, Win32/chirB, an email worm that sends itself to email addresses stored on the infected computer.

For the sake of analysis, IDC chose to assume that 20% of active malware programs could infect *just one other computer*. Since this includes malware re-infections on the same computer – in which an infection that was considered cleaned or quarantined comes back – it seems to be a lower bound for the possibility of multiple infections from the same piece of malware.

HOW DOES THIS AFFECT YOU?

Whether you are knowingly or, unfortunately, *unknowingly* using pirated software, you will indubitably come face to face with malware somewhere along the way. In our survey, consumers indicated clearly that they both (1) had experienced security problems with some software they had acquired in the last two years and (2) knew what they feared about those security issues.

Respondents also told us that 54% of the people they knew who used *pirated* software had experienced security problems.

[11] Cisco, Ibid.

[12] http://www.microsoft.com/en-us/news/stories/cybercrime/index.html

What do consumers fear from malicious code? Figure 8 tells you.

FIGURE 8

The Biggest Fears from Infected Pirated Software

n = 951 consumers

Up to three responses allowed

Source: IDC, 2014

These fears are well founded. Using data from the survey and the National University of Singapore forensic work, we can come up with an estimate of the cost to consumers from malware in pirated software. These costs include:

- The value of time lost dealing with issues[13]
- The cost of paying professionals to help fix the problem
- The cost to replace lost data or re-establish an identity after identity theft

Note that there was no attempt to fix a value to lost data (e.g., photos, documents, personal records, etc.), no estimate of losses from fraud, and no estimate of losses or litigation from identity theft. Taking these impacts into account would only add to the costs estimated by IDC.

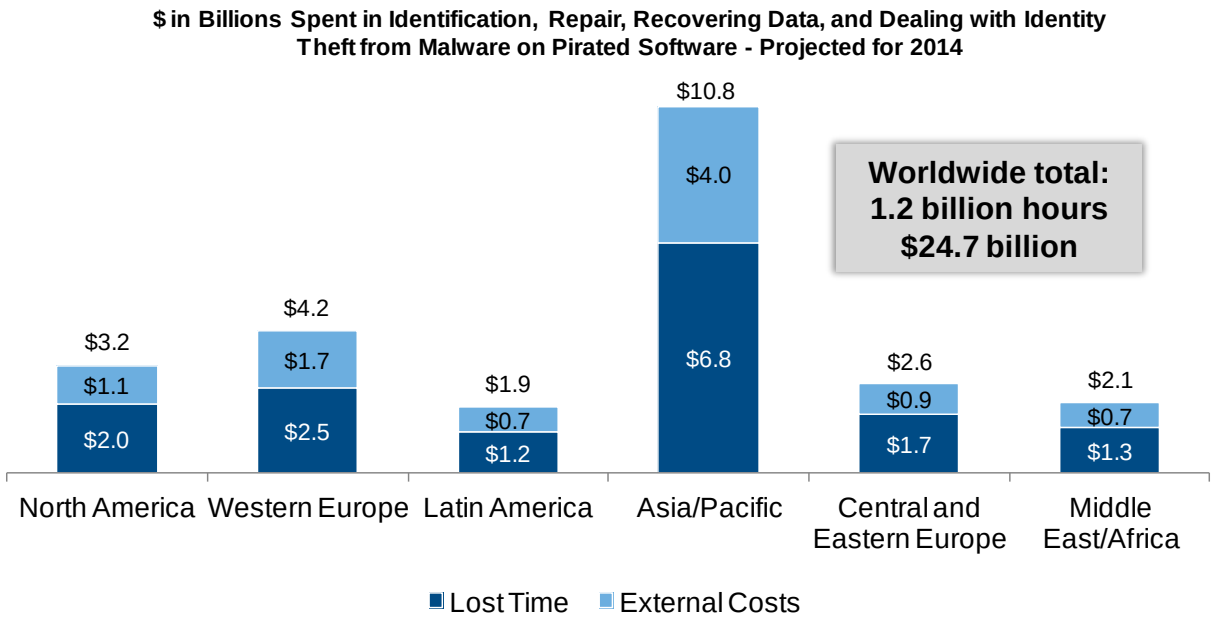
[13] For the sake of quantifying the value of the time lost dealing with security issues, we chose the average hourly wage in a country. Economists will argue that lost personal hours lost don't always or even often equate to lost wages, but it seemed a reasonable way to quantify the unasked question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

Figure 9 shows the cost breakdown to consumers by region. Note that (1) total costs 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 mature markets because more software is pirated there (65% of pirated software), and (3) these figures are averages.

The total? $24.7 billion and 1.2 billion wasted hours.

FIGURE 9

Consumers' Costs from Infected Pirated Software



Note: totals may not add because of rounding.

Source: IDC Economic Impact of Pirated Software Malware Model, 2014

Since this analysis is built on average time and money spent, the reality is that the per-pirated-software-program costs may vary dramatically. For instance, the time to fix problems in the model is estimated using the mean of responses from all the surveyed countries. However in some cases a sizable portion of respondents estimated times more than 3-5 times the average.

For identity theft, the disparity between the average and the possible is stark. According to the United States Department of Justice, in 2012 half of identity theft victims were able to deal with the associated problems in less than a day. But for 10% of them it took more than a month. Nearly 50% lost less than $100, but more than 15% lost more than $1,000.[14]

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.

[14] *Victims of Identity Theft, 2012* www.bjs.gov/index.cfm?ty=pbdetail&iid=4821

ENTERPRISES HAVE EVEN MORE TO LOSE

Enterprises have an advantage over consumers in that they have IT professionals to protect their IT assets and budgets for computer security. But they are also handy targets with more valuable data on their computers.

And targets they are:

- According to the Cisco 2014 Annual Security Report, threat alerts grew 14% in 2013.[15]
- In its annual global study of computer security breaches,[16] Verizon found that 40% of "threat events" involved malware, 71% targeted end-user devices, 92% were initiated by outsiders, and 75% were conducted for financial motives.
- According to a Trend Micro report,[17] threats to the online banking industry alone surpassed 200,000 in 2013, the highest number ever. And in two paragraphs the report described four actions that exposed more than 300 million log-on credentials to online Internet commerce customer accounts.
- Perhaps the biggest news of 2013 was the breach of 110 million credit cards and personal credentials of Target customers, caused by criminals using malware on Target servers to extract customer and credit card data from POS terminals. This single breach cost Target $400 million in lost holiday sales (and $200 million in earnings) in 2013,[18] and will cost millions in remediation and millions more in legal costs as Target looks to defend a minimum of 40 lawsuits.
- In the IDC survey, 28% of respondents reported security breaches causing network, computer, or Web site outages occurring every few months or more. 65% of outages involved malware on end-user computers.

WHAT ARE THE COSTS FOR ENTERPRISES?

Consumers may acquire more pirated software than enterprises, but enterprises face more risks with the pirated software they do acquire.

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

- Labor costs associated with preventing or identifying and rectifying security problems
- Costs of third-party support to deal with the problem
- Employee downtime
- Costs to locate and reinstall lost data

[15] Cisco, ibid.

[16] *2013 Data Breach Investigations Report,* www.verizonenterprise.com/DBIR/2013/

[17] www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-trend-micro-security-predictions-for-2014-and-beyond.pdf

[18] Based on Target statements that the breach caused the company to lower earnings estimates for the fourth fiscal quarter from $1.50-$1.60 per share to $1.20-$1.30 and a quarter over prior year quarter sales decline of 2.5%. pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance

- Costs of data loss from theft as a result of planted malware
- Costs of fraud from theft of credentials or customer records
- Losses – in terms of revenue, time, and operational cycles – from Website, network, and computer outages
- Cost of resources supporting users with stolen credentials

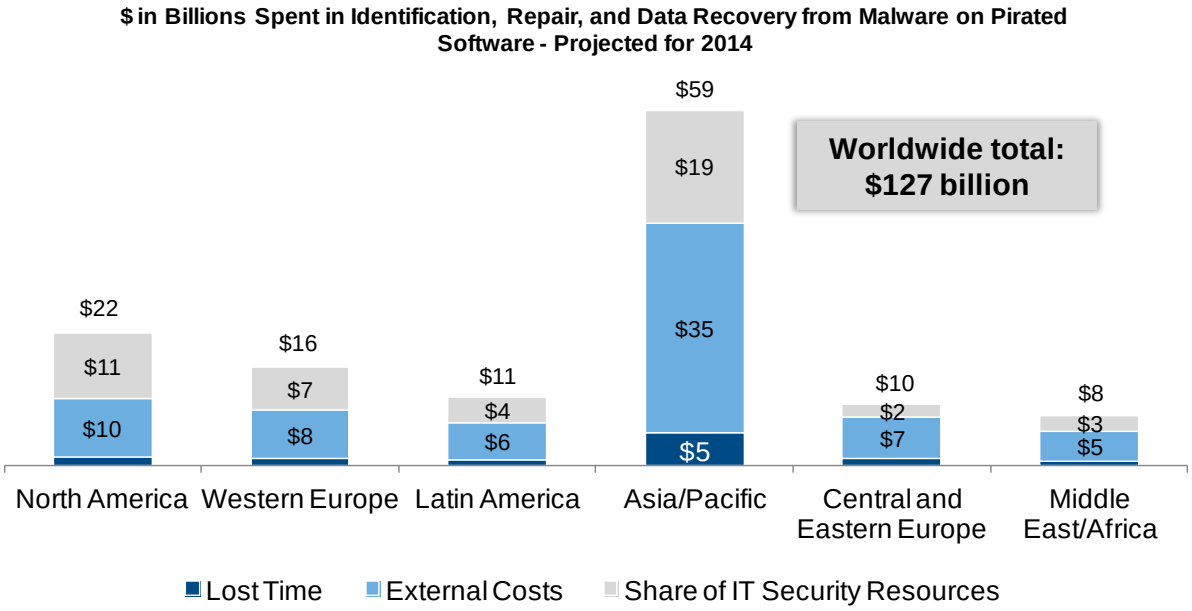
And this doesn't even cover the costs of replacing pirated software with legitimate software, going through a software audit, or facing fines when caught with pirated software.

So what exactly is this costing enterprises? As we did for consumers, IDC used information on piracy rates, information security spending, National University of Singapore forensic results, and survey information to estimate the direct costs to enterprises from malware associated with pirated software. These direct costs include labor, external spending, and a small share of IT security infrastructure.

Figure 10 provides those costs by region. The total is $127 billion.

FIGURE 10

The Cost to Enterprises from Infected Pirated Software



Note: totals may not add because of rounding.

Source: IDC Economic Impact of Pirated Software Malware Model, 2014

The costs are highest in Asia Pacific, despite the fact that labor costs are so much lower than the developed world, simply because of the sheer amount of pirated software there. Asia Pacific encompasses 40% of the world's installed base of enterprise PCs and 60% of pirated enterprise software units – not counting the ones brought to work by end users.

THE COST OF DATA BREACHES

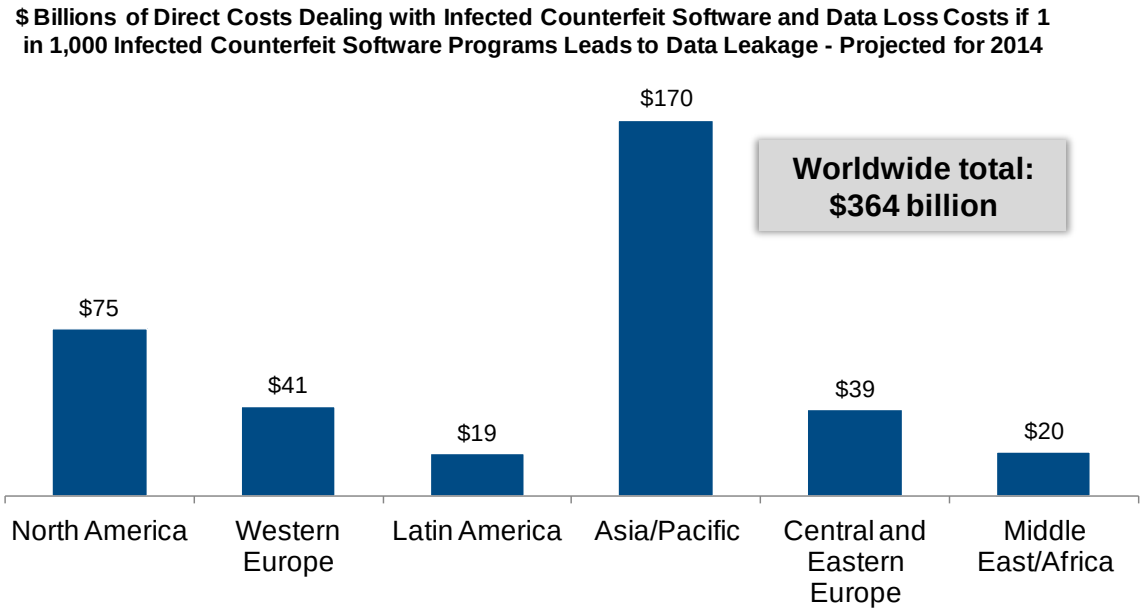
For enterprises, the threat from pirated software is simple enough: it is the prevalence of malware and the costs to deal with it. But the connectedness of enterprise computers, and the purpose of some of that malware – information theft, including passwords, account credentials, and access codes – means that enterprises have exposure far beyond the costs to clean an end user's infected computer.

But what's the cost of a data breach? Last year, according to the Ponemon Institute Benchmark Study[19], the cost per lost record in the U.S. was $194. This year it is $188. But on a worldwide level, the average cost went up from $130 to $136. For data breaches that are the result of malicious attacks, the costs are higher: $157 per leaked record globally, $277 in the United States.

Using these costs and other data from the Ponemon study, IDC market data, and the survey and forensic research, IDC estimates costs to enterprises from data breaches in 2014 as shown in Figure 11. The total? $364 billion and 2.3 billion lost records.

FIGURE 11

Potential Cost to Enterprises from Lost Data



Source: IDC Economic Impact of Pirated Software Malware Model, 2014

Added to the direct costs of dealing with malware from pirated software we come up with a global total for losses to enterprises of $491 billion.

[19] From the *2013 Cost of Data Breach Study: United States* and the *2013 Cost of Data Breach Study: Global Analysis*, published by Ponemon Institute http://www.ponemon.org/library/2013-cost-of-data-breach-global-analysis

REGIONAL DIFFERENCES

Note that this paper includes many regional findings in figures located throughout, and a complete set of data tables is provided in the appendix. In addition, there are some key regional differences worth highlighting:

- Not surprisingly, infection rates are higher in emerging markets, where more consumers and enterprises acquire software and PCs from suspect sources – small specialty shops, street markets, consultants, etc.– at higher rates than in mature markets. For instance, China, Thailand, and Mexico had the highest rate of PC infections and of infections of software bundled with PCs.
- Because of higher rates of piracy in emerging markets, while only 40% of PCs are used in Asia/Pacific, IDC estimates that Asia/Pacific will account for 47% of the world's pirated software in 2014. Because of higher infection rates, IDC estimates that it will account for 60% of all *infected* pirated software.
- This higher infection rate and higher number of pirated software units is why the economic losses hit Asia Pacific so hard, despite lower labor costs to deal with pirated software. The Asia Pacific region will incur more than 40% of worldwide consumer losses and more than 45% of the world's enterprise losses from malware on pirated software
- On the other hand, the wealthier regions – North America and Western Europe – are more likely to be targets for cybercrime and in those regions the cost of dealing with data breaches is higher per record. In the survey, respondents from the United States and from Western Europe estimated that 24% and 25% of their system, network, or web site outages were caused by cybercriminals respectively, while those from Asia Pacific, Latin America, and Central and Eastern Europe had lower estimates (18%, 18%, and 16% respectively)
- The wealthier regions also saw fewer workers installing their own software unbeknownst to the organization. In North America only 3% said they did so with 11% in Western Europe, while in Asia Pacific and Latin America, the figures were higher than 30%.

NATIONS AT RISK

Given the impact on consumers and enterprises from malware associated with pirated software, it's easy to draw implications for governments, as they are users of software and victims of security attacks, too. But they have the added burden of dealing not only with the consequences of their attentiveness – of lack of it – to the security risks of using pirated software, but also of the consequences of the actions of their citizens and industries.

Further, governments must deal with issues of national security. The data from our survey show that cybersecurity is top of mind for most government officials. Critical infrastructure is at stake, as is confidential government information.

The question is do governments understand the link between potential security breaches and software piracy?

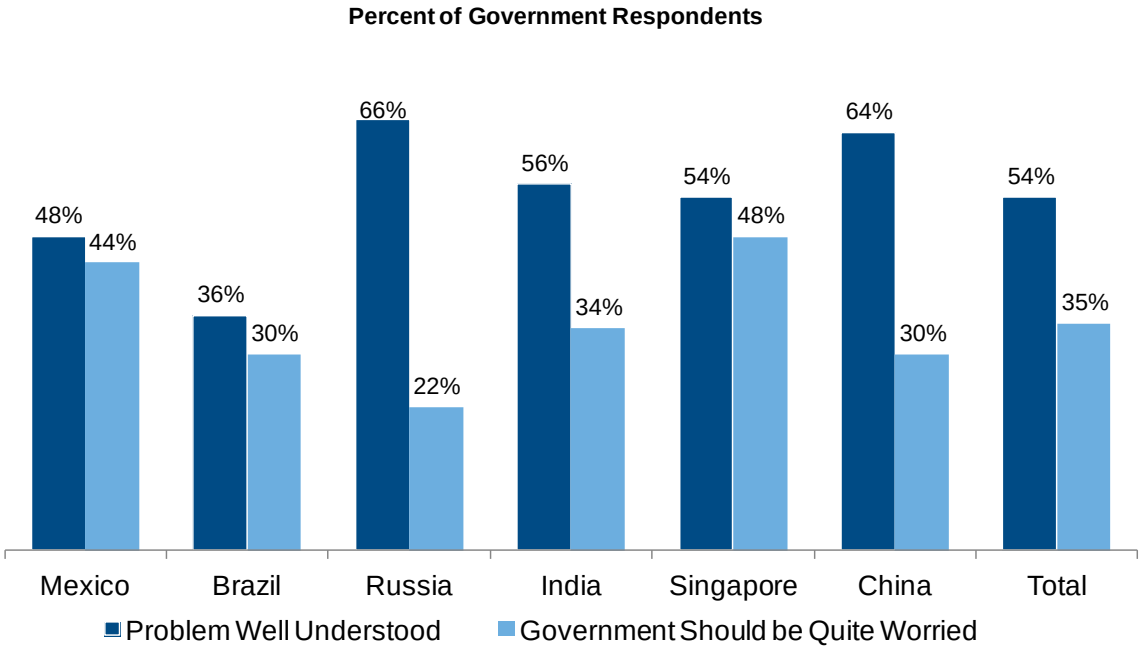
The 302 government officials surveyed indicated that, to some extent, they do. In total 54% said that the connection is well understood. In Latin America, that awareness dropped to 42%, while in Central and Eastern Europe it was 66%.

Furthermore, 35% of government respondents said their governments should be quite worried about it. On the other hand, 26% said their governments either don't need to worry at all or need to worry only a little bit.

Figure 12 shows the knowledge and worry level by country.

FIGURE 12

Knowledge and Worry Level by Country



n = 302 government officials

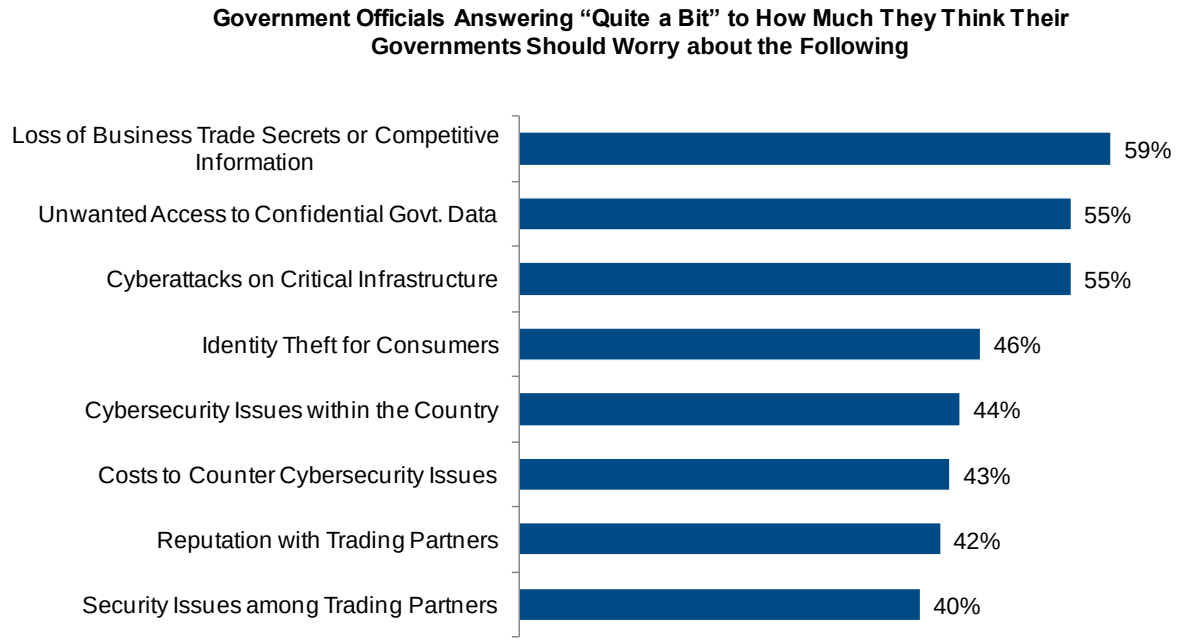
Note: Respondents were asked how well understood the linkage between pirated software and infections. The figure shows those respondents who rated "well understood." They were also asked how worried their government needs to be about malware and the figure shows those who responded "quite worried."

Source: IDC, 2014

Figure 13 displays what respondents said they *do* worry about when it comes to the cybersecurity threats stemming from the use of pirated software. Some threats affect the government itself, some affect businesses or consumers.

FIGURE 13

Government Worries



n = 302 government officials

Source: IDC, 2014

There is some good news. 48% of respondents reported that, at some level of government, be it local, regional, or central, they were aware of government advisories warning about the problem of malware on pirated software.

Some of the knowledge may be personal: 16% of the officials surveyed reported that they had had problems with software in the last two years, including viruses, crashes, slowdowns, and lost files. But some of it should be institutional. IDC estimates that governments, as users of PCs and software, will themselves lose more than $50 billion in 2014 from the costs of dealing with malware on pirated software. This is in addition to costs for potential lost data.

INTO THE HANDS OF CYBERCRIMINALS

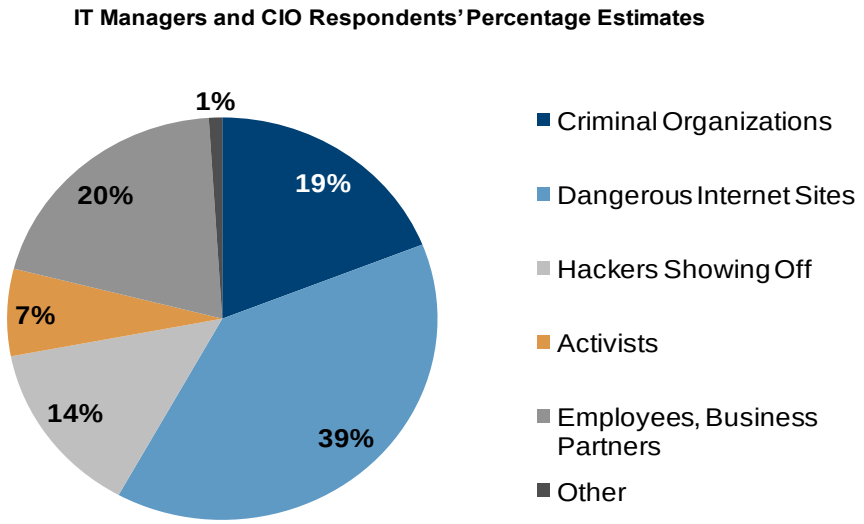
Most malware is propagated by cybercriminals, as is most pirated software. A review of our survey and of external security-oriented literature indicates that somewhere between 19% (the figure arrived at in the IDC survey) and 55% (as estimated by Verizon) of security attacks emanate from criminal organizations.

But even these estimates may be low.

Figure 14 shows what our survey respondents felt was the cause of their system, network, and Web site outages.

FIGURE 14

Sources of System, Network, or Web Site Outages



n = 450 CIOs/IT managers

Source: IDC, 2014

Look a little closer. The biggest category is dangerous Internet sites (Web, social network or commerce sites). Isn't some of the malware lurking on them likely to have been put there by criminals? And what about activists? If they release personal data to make a point, would they, then, be criminals?

The Verizon research attributes 92% of external breaches to external actors and 55% of that to organized crime (with 13% from unknown sources). And 75% of threat activity is driven by financial motives. Are any of those creating security threats for profit *not* criminals?

And Cisco reports that in a recent project looking at Domain Name Service (DNS) look-ups, its experts found that in every case organizations showed evidence that their networks had been misused or compromised. 100% of the business networks analyzed had traffic going to websites that host malware, 92% showed traffic to Web pages without content (which typically host malicious activity), and 96% showed traffic to hijacked servers.

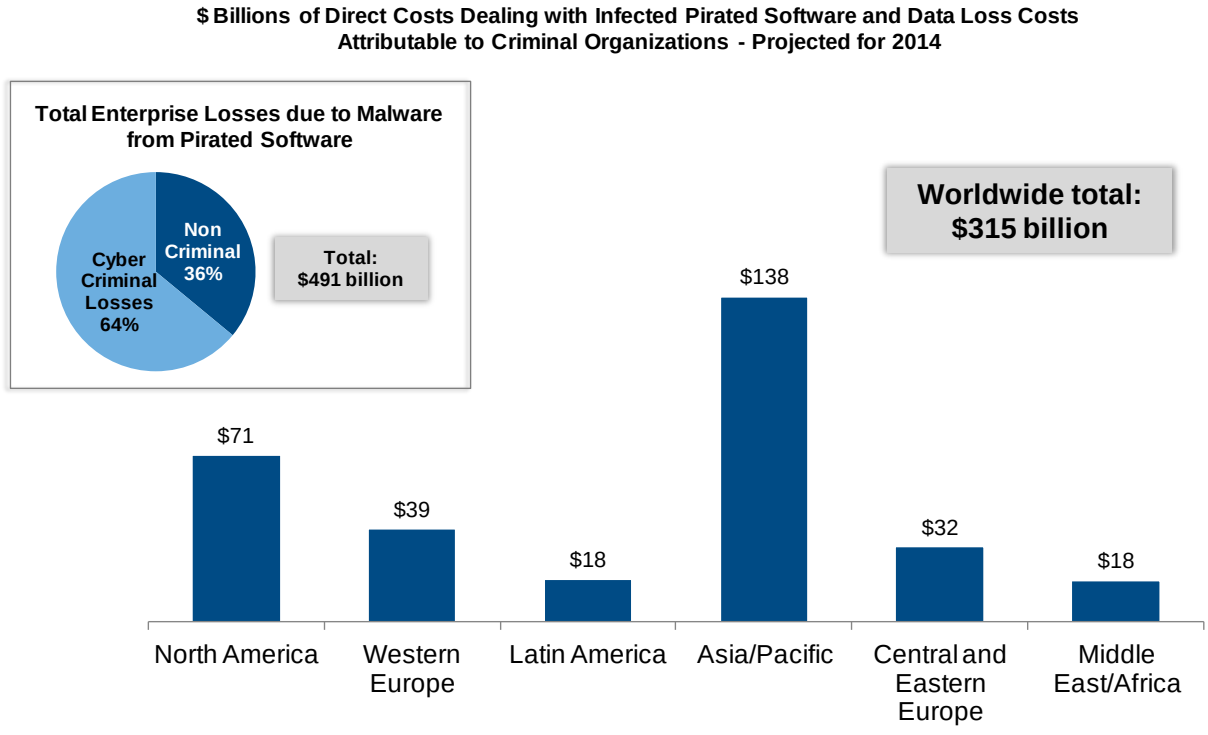
In other words, criminals are everywhere in cyberspace, trying to get our data.

In our economic model, then, we chose a conservative approach to allocating malware infection to cybercriminals, averaging the Verizon percent with our survey respondent percent. We did, however, assume that costs were higher to deal with each instance of infection when the malware was created by criminals.

Figure 15 shows the costs – in remediating or preventing security events and dealing with data breaches – we think are directly attributable to criminal organizations: $315 billion, or 64% of total enterprise losses

FIGURE 15

Losses to Enterprise from Cybercrime



Note: totals may not add because of rounding.

Source: IDC Economic Impact of Pirated Software Malware Model, 2014

In addition to out-of-pocket costs, what specific harm was done from the security breaches reported by survey respondents?

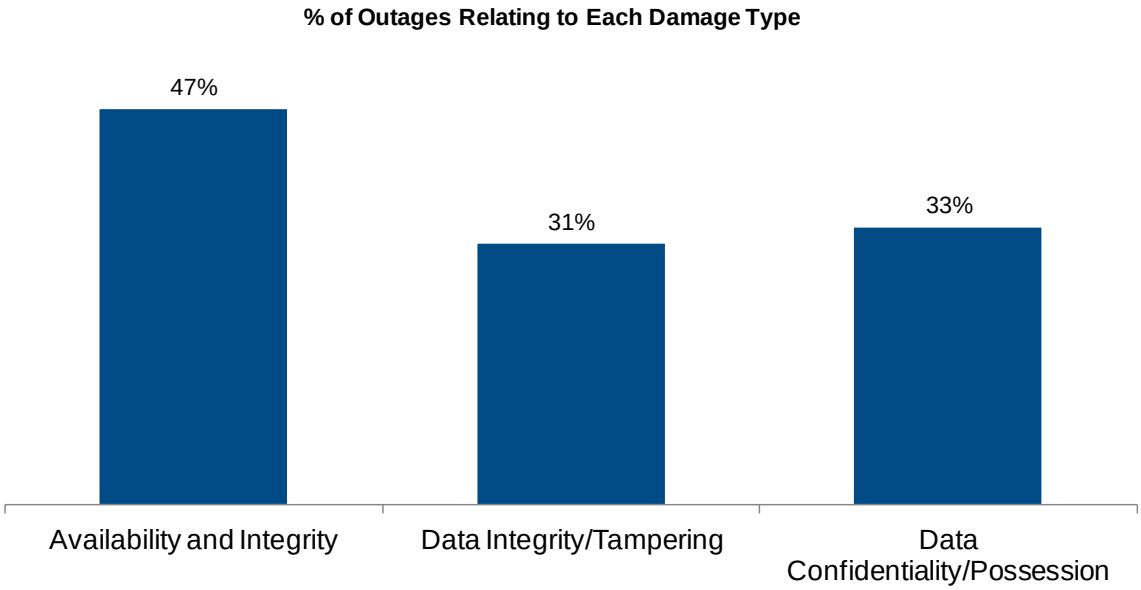
Using a threat assessment developed by Verizon and used by a number of law enforcement agencies, consulting and security firms, and major customers, we asked respondents to assign types of damage resulting from their security outages. These fell into three categories:

- Data confidentiality or possession – e.g., data was observed by hackers or stolen and/or sensitive records accessed.
- Integrity and authenticity – data or software had been altered or compromised, e.g. Web sites defaced, privileges modified, or log tampering occurred.
- Availability and utility – data or equipment were no longer available or performance had slowed, e.g., from denial of service attacks, spam attacks, or blocked or hijacked access.

Figure 16 shows the results. Note that the sum adds to more than 100%, since one outage can do damage in multiple ways.

FIGURE 16

Damage from Security Breaches



n = 450 CIOs/IT managers

Source: IDC, 2014

Of course, enterprises aren't the only entities subject to cybercriminals. Remember the Citadel botnet? While 64% of the enterprise losses from malware on pirated computers come from cybercriminal activity, IDC estimates that 49% of consumer losses, or $12 billion, come from cybercriminals. About half of that is from identity theft.

FUTURE OUTLOOK AND CALL TO ACTION

The bad news is unless the use of pirated software declines, the security threats and potential losses to consumers and enterprises will go up. Security systems are getting better, but the criminal creators of malware are getting more sophisticated at the same time. Don't expect the environment to get less contagious, or an antivirus program to be a magic pill. The security risks faced by users of pirated software can only increase.

The good news is that cutting the use of pirated software is a straightforward exercise. So is running frequent security updates, monitoring the use of software installed in enterprises by employees, and buying a PC from a trusted source. Cut piracy and you cut your exposure to risk, data loss, and financial loss.

The losses we chart here are a lot larger than the price tag of the legitimate software it would take to replace the entire world's pirated software.

But pursuing these practices is an individual decision. Piracy rates may drop across the world over the next few years, but the growth in demand for software will probably mean more actual pirated copies of software will be available.

Why should a consumer spend a month straightening out affairs after his or her identity has been stolen if buying legitimate software makes that unnecessary? Why should an enterprise spend the equivalent of more than 10% of its IT labor costs dealing with the issues brought about by malware, along with $157 for every data record lost from a malware-induced security incursion if it can spend a lot less buying legitimate software and enforcing a policy for its use?

The best prevention for the problems and losses we have charted here is this: use the genuine item. That means trusted and secure operating systems and applications.

There are other specific imperatives for all those concerned about cybersecurity.

- Consumers shouldn't fall into the trap of thinking pirated software is "free," and should worry about online safety and security. They also need to be on the lookout for software that looks or appears legitimate but isn't, perhaps because it has an uncharacteristic price, whether they buy it from a computer store, an online site, or with a PC. They also need to understand the risks of using pirated software beyond the risk of violating copyright laws and must be vigilant in running security scans.
- Enterprises have a lot to lose from cybersecurity breaches and thus need to appreciate the value of Software Asset Management (SAM) to improve IT governance & compliance in the organization. They should use legitimate and secure software and periodically undertake software & cybersecurity audits. They should enforce strong IT procurement and usage policy measures company-wide, monitor the unauthorized piracy-related activities of their employees, and make their vendors and partners adopt and adhere to Clean IT practices in their supply chains.
- Governments need to be pro-active in educating their populations and government departments on the cybersecurity and malware threats from software piracy. They need to be fully aware and sensitized to the dangers to sensitive government information, government services, and critical infrastructure if they have a non-genuine software environment. When it comes to cybersecurity,

governments need to behave like responsible enterprise users. They also need to ensure that they have a strong detection and enforcement infrastructure for preventing intellectual property theft and cybersecurity abuses, and for pursuing cybercriminals.

- Computer and software resellers have to acknowledge their important point-of-sale role in safeguarding the information security of their customers by selling only legitimate software. They need to understand that by offering their customers installation of pirated software, they might be putting those customers in the hands of cybercriminal organizations. It is equally important for them to trust only authorized or recommended sources in the upstream supply chain and stay away from "sweet" deals. Piracy also could make them civilly and criminally liable, which can be very damaging.
- PC hardware manufacturers (OEMs) have to understand their critical role in preventing cybersecurity breaches against their customers and how that can help protect their PC brand image. Good software and hardware are two sides of the same coin. At a minimum, it is important that new computer shipments come pre-installed with genuine and legal operating systems. If more consumers find PCs on sale which do not have trusted and secure software, they will inadvertently be drawn towards the piracy option, which impacts the entire IT ecosystem.

There is work to be done for all. With billions at stake.

SIDEBAR: MICROSOFT'S CYBERCRIME CENTER

Launched in November 2013, the Microsoft Cybercrime Center in Redmond, WA is home to the Digital Crimes Unit (DCU). The DCU is comprised of more than 100 attorneys, investigators, business professionals, and forensic analysts based in North America, EMEA, Asia/Pacific, India, China, and Latin America. DCU focuses on combating issues such as malicious software, including malware and botnets; IP crimes, including software piracy and counterfeiting; and technology-facilitated online child exploitation.

Microsoft Cybercrime Center's combination of talent and forensic and analytical tools marks a new era for Microsoft in fighting cybercrime. Through partnerships with international law enforcement agencies and other industry experts, the Microsoft Cybercrime Center works to better protect consumers online and ensure that people worldwide can use their computing devices and services with confidence.

Readers can find a video about the cybercrime center here:
http://www.microsoft.com/government/ww/safety-defense/initiatives/Pages/cybercrime-center.aspx

APPENDIX – METHODOLOGY

National University of Singapore Forensic Analysis

The first step of the forensic analysis consisted of securing the PCs and software media for the study. The National University of Singapore team gathered a total of 203 personal computers and laptops from 11 countries: Brazil, China, India, Indonesia, Mexico, Russia, South Korea, Thailand, Turkey, Ukraine, and the United States. These samples were purchased from the target countries on a random basis from PC and software vendors. The purchases were performed by independent investigators

who acted as "normal walk-in customers" with the goal of coming across as students, young professionals, home makers, and small business owners.

Once these samples were collected, the team created an image of the hard disk from each of the samples. The team then performed malware detection by of scanning each of the samples with anti-virus software. For this study, five anti-virus engines were used: Avira, AVG, Avast, Microsoft Security Essentials, and Kaspersky. The team then investigated each system to detect changes to the system settings during operating system installation or by malware. Finally, the team analyzed the run-time behavior of the samples for signs of malicious behavior.

IDC Surveys

During December of 2013 IDC conducted three global surveys, one of consumers and workers, one of CIOs/IT managers, and one of government officials. The consumer/worker survey consisted of 951 responses, and the CIOs/IT professionals consisted of 450 respondents from 15 countries: Brazil, China, India, Indonesia, France, Germany, Japan, Mexico, Poland, Russia, Singapore, Thailand, Ukraine, United Kingdom, and the United States. The government survey consisted of 302 government officials from six countries: Brazil, China, India, Mexico, Russia, and Singapore.

In the CIO/IT manager sample, 35% came from organizations with more than 1,000 employees, 65% from smaller organizations. In the survey of consumers/workers, 46% worked at organizations with more than 1,000 employees and 54% at smaller organizations. The industry mix in both surveys was representative of the general economies. In the government survey, 54% were from central government, 23% from regional, 19% from local governments, and 5% from independent agencies.

The surveys were conducted via Internet using third party panels of computer users. Note that in figures referring to survey data where we break out regions, the label "World" means the unweighted total of all respondents.

Economic Impact Modeling

To develop the economic impact figures in this White Paper, we developed a Dangers of Counterfeit Software Model that incorporated proprietary data from the IDC BSA | The Software Alliance 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. To complete the picture we developed rest-of-region estimates to complete the global picture.

The "chance of infection" estimates we developed 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, 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., % of pirated software resulting from misuse of volume licensing).

This done, we had a picture of the number of counterfeit units of software for 2014 and what % would be infected. The next step was to estimate what % of the infections would be routinely caught by user and enterprise anti malware software without requiring any further action. Here we used the % 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 them 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 % 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, anti-malware software, etc.) that would apply to malware from counterfeit software.

Altogether, these 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.

APPENDIX – REGIONAL DATA TABLES

TABLE 1

PCs from Suspect Sources*: % Not Buying PCs Directly from Name Brand Vendors or National Stores

	NA	WE	LATAM	AP	CEE	TOTAL
Consumers	62%	59%	48%	68%	53%	65%
Enterprises	23%	26%	29%	33%	29%	30%

* includes computer specialty shops, consultants, non-branded PC assembler, gifts, online store/trading portal, auction sites, flea markets, yard sales, and self-built

Source: IDC, 2014

TABLE 2

Inattention to Security Updates: % Not Installing Updates (Consumers) or % with No Regular Process to Install Security Updates (CIOs/IT Managers)

	NA	WE	LATAM	AP	CEE	TOTAL
Consumers	39%	45%	36%	41%	53%	43%
Enterprises	19%	35%	23%	22%	30%	26%

n = 951 consumers, 450 CIOs/IT managers

Source: IDC, 2014

TABLE 3

BYO Pirated Software: % of Employees Installing Their Own Software without the Enterprise Knowing on Work Computers Within the Last Two Years

	NA	WE	LATAM	AP	CEE	TOTAL
Employees	3%	11%	38%	32%	22%	27%

n = 951 consumers/employees

Source: IDC, 2014

TABLE 4

Problems with User-installed Software at Work (Enterprise)

	NA	WE	LATAM	AP	CEE	TOTAL
None	21%	32%	17%	19%	50%	25%
Increases cost to support that PC	29%	15%	32%	27%	10%	24%
Increases drain on IT resources	36%	16%	29%	36%	15%	29%
Increases the threat of security issues	50%	47%	48%	53%	42%	51%
Interferes with authorized software	21%	22%	31%	23%	4%	20%

n = 450 CIOs/IT managers

Note: multiple responses allowed

Source: IDC, 2014

TABLE 5

Problems with Pirated Software (Consumers)

	NA	WE	LATAM	AP	CEE	TOTAL
Wouldn't run, had to reinstall	19%	24%	15%	27%	27%	25%
Worked for a while then stopped	25%	19%	14%	22%	13%	19%
Infected the computer with a virus*	11%	11%	19%	27%	19%	21%
Overran my computer with pop-up ads*	25%	15%	18%	26%	20%	22%
Really slowed down my computer, had to uninstall*	25%	29%	37%	45%	38%	39%
Made my home network slower	36%	19%	23%	25%	12%	22%
Destroyed my files, photos, videos, music etc.*	22%	7%	3%	14%	5%	10%
Corrupted the hard-drive that I had to reformat*	19%	6%	9%	13%	3%	10%
My email or Facebook or bank account got hi-jacked*	0%	6%	4%	6%	5%	5%
Never had a problem	28%	42%	39%	25%	39%	32%

n = 951 consumers

* indicative of Malware

Note: multiple responses allowed

Source: IDC, 2014

TABLE 6

Problems with MS Office Installed on Older PCs (Enterprises)

	NA	WE	LATAM	AP	CEE	TOTAL
Had no Problem	77%	90%	68%	64%	81%	73%
Couldn't install	14%	9%	14%	19%	16%	15%
Couldn't activate, needed to obtain activation keys	18%	12%	30%	27%	17%	22%
Discovered malware in the product	14%	7%	21%	23%	4%	16%
Discovered hadn't been properly licensed	5%	6%	12%	29%	19%	19%

n = 450 CIOs/IT managers

Note: multiple responses allowed

Source: IDC, 2014

TABLE 7

Biggest Fear from Infections (Consumers)

	NA	WE	LATAM	AP	CEE	WORLD
Time and cost to disinfect	42%	25%	34%	32%	20%	30%
Potential identity theft	39%	55%	47%	47%	42%	47%
Unauthorized Internet transactions and online fraud	54%	55%	54%	48%	50%	51%
Loss of data, files, or private information	46%	50%	56%	65%	63%	60%
Hi-jacking of email, social networking, bank accounts	39%	58%	50%	45%	57%	50%
Effect on PC performance - E.G., frequent computer crashes	42%	19%	29%	37%	33%	32%
Might infect other PCs at work, home, etc.	7%	13%	21%	18%	11%	15%
Not worried about PC becoming infected	11%	8%	3%	3%	8%	5%

n = 951 consumers

Note: multiple responses allowed

Source: IDC, 2014

TABLE 8

Biggest Fear for the Country from Infectious Malware in Pirated Software (Government Respondents)

	LATAM	AP	CEE	Total
Cyberattacks on Critical Infrastructure	56%	56%	50%	55%
Loss of Business Trade Secrets or Competitive Information	68%	55%	52%	59%
Unwanted Access to Confidential Government Data	57%	57%	46%	55%
Identity Theft for Consumers	50%	45%	42%	46%
Cybersecurity Issues within the Country	46%	45%	36%	44%
Cybersecurity Issues between Trading Partners	40%	44%	30%	40%
Cost to Government to Counter Cybersecurity Issues	46%	42%	38%	43%
Impact on Country's Reputation with Trading Partners	45%	42%	34%	42%

n = 302 government officials

Percentages indicate those answering "quite a bit" – the highest score allowable – to how worried the government should be.

Source: IDC, 2014

TABLE 9

How Well is the Connection Between Pirated Software and Malware Understood in the Government?

	LATAM	AP	CEE	TOTAL
Not well or only somewhat understood	58%	42%	34%	46%

n = 302 government officials

Source: IDC, 2014

TABLE 10

How Worried Should the Government Be About Malware on Pirated Software Being Planted by Criminal Organizations?

	LATAM	AP	CEE	TOTAL
Quite worried (highest score)	37%	37%	22%	35%

n = 302 government officials

Source: IDC, 2014

TABLE 11

Government Education on Security Threats from Pirated Software

	LATAM	AP	CEE	TOTAL
Aware of any information, guidance, advisory, memo published by your government — central, provincial, or local — on the linkage between the use of pirated software and cybersecurity threats from malware	35%	58%	46%	48%

n = 302 government officials

Source: IDC, 2014

TABLE 12

Frequency of Outages (Enterprises): How Often Does Your Organization Have Network, Web Site, or Individual Computer Outages as a Result of IT Security Issues?

	NA	WE	LATAM	AP	CEE	TOTAL
Every Few Months or More	30%	26%	25%	29%	30%	28%

n = 450 CIOs/IT managers

Source: IDC, 2014

TABLE 13

Cause of Outages (Enterprises)

	NA	WE	LATAM	AP	CEE	TOTAL
Denial of service attacks	41%	30%	40%	38%	32%	36%
Cyberhacking	30%	19%	21%	33%	25%	28%
Viruses or malware on end user computers	48%	59%	77%	66%	66%	65%
Viruses or malware infections from suppliers or distributors	30%	30%	28%	33%	22%	30%
Other	7%	7%	4%	3%	3%	4%

n = 450 CIOs/IT managers

Note: multiple responses allowed

Source: IDC, 2014

TABLE 14

Sources of Outages (Enterprises)

	NA	WE	LATAM	AP	CEE	TOTAL
Cyber Criminal organizations or individual criminals	24%	25%	18%	18%	16%	19%
Dangerous websites, social networks, online trading sites, etc.	40%	45%	43%	33%	47%	39%
Hackers intent on mischief or showing off	19%	14%	13%	13%	13%	14%
Cyber Activists	6%	3%	9%	9%	8%	7%
Internal employees, business partners, or others you deal with	9%	13%	17%	27%	13%	20%
Other	3%	0%	1%	0%	3%	1%

n = 450 CIOs/IT managers

Note: totals may not add because of rounding.

Source: IDC, 2014

TABLE 15

Impact of Cybersecurity Events (Enterprises)

	NA	WE	LATAM	AP	CEE	TOTAL
Data confidentiality or possession – e.g., data was observed by hackers or stolen, sensitive records accessed, etc	26%	38%	37%	33%	29%	33%
Integrity and authenticity – data or software has been altered or compromised, e.g. Web site defaced, privileges modified, log tampering	35%	22%	34%	31%	38%	31%
Availability and utility – data or equipment are no longer available or performance has slowed, e.g., from denial of service attacks, spam attacks, blocked or hijacked access	54%	54%	39%	46%	49%	47%

n = 450 CIOs/IT managers

Note: multiple responses allowed

Source: IDC, 2014

TABLE 16

Consumer Costs Dealing with Malware in Pirated Software ($B)

	NA	WE	LATAM	AP	CEE	MEA	WORLD
Internal (Labor)	$2.0	$2.5	$1.2	$6.8	$1.7	$1.3	$15.6
External Costs	$1.1	$1.7	$0.7	$4.0	$0.9	$0.7	$9.1
Total Costs	$3.2	$4.2	$1.9	$10.8	$2.6	$2.1	$24.7

Note: totals may not add because of rounding.

Source: IDC Economic Impact of Pirated Software Malware Model, 2014

TABLE 17

Enterprise Costs Dealing with Malware in Pirated Software ($B)

	NA	WE	LATAM	AP	CEE	MEA	WORLD
IT Labor	$1.5	$1.2	$0.9	$5.3	$1.0	$0.8	$10.7
External Costs	$9.7	$7.9	$6.2	$35.0	$7.0	$5.0	$70.9
Share of IT Resources	$10.8	$7.1	$4.1	$18.6	$2.2	$2.5	$45.4
Total Costs	$22.0	$16.2	$11.2	$59.0	$10.3	$8.3	$126.9

Note: totals may not add because of rounding.

Source: IDC Economic Impact of Pirated Software Malware Model, 2014

TABLE 18

Enterprise Costs Dealing with Data Breaches ($B)

	NA	WE	LATAM	AP	CEE	MEA	WORLD
If 1/1000 pirated software packages with malware lead to a breach	$75	$41	$19	$170	$39	$20	$364

Source: IDC Economic Impact of Pirated Software Malware Model, 2014

TABLE 19

Total Enterprise Costs from Malware in Pirated Software ($B)

	NA	WE	LATAM	AP	CEE	MEA	WORLD
Costs	$97	$57	$30	$229	$49	$28	$491

Source: IDC Economic Impact of Pirated Software Malware Model, 2014

TABLE 20

Costs from Cybercrime Related to Malware in Pirated Software ($B)

	NA	WE	LATAM	AP	CEE	MEA	WORLD
Enterprise Direct and Indirect Costs	$13	$10	$6	$30	$6	$4	$69
Enterprise Lost Data	$57	$30	$12	$108	$26	$13	$246
Total	$71	$39	$18	$138	$32	$18	$315
% Total Enterprise Losses	72%	69%	61%	60%	65%	62%	64%

Note: totals may not add because of rounding.

Source: IDC Economic Impact of Pirated Software Malware Model, 2014

TABLE 21

National University of Singapore PC Infection Data

	NA	LATAM	AP	CEE	MEA	WORLD
% PCs From Channel with Malware	31%	67%	68%	61%	35%	61%
Discrete Threats per PC	1.8	2.6	4.1	1.3	1.3	3.0

Source: National University of Singapore forensic analysis, 2014

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com