



INFORMATION, COMMUNICATION AND ENTERTAINMENT

An Inconvenient Reality

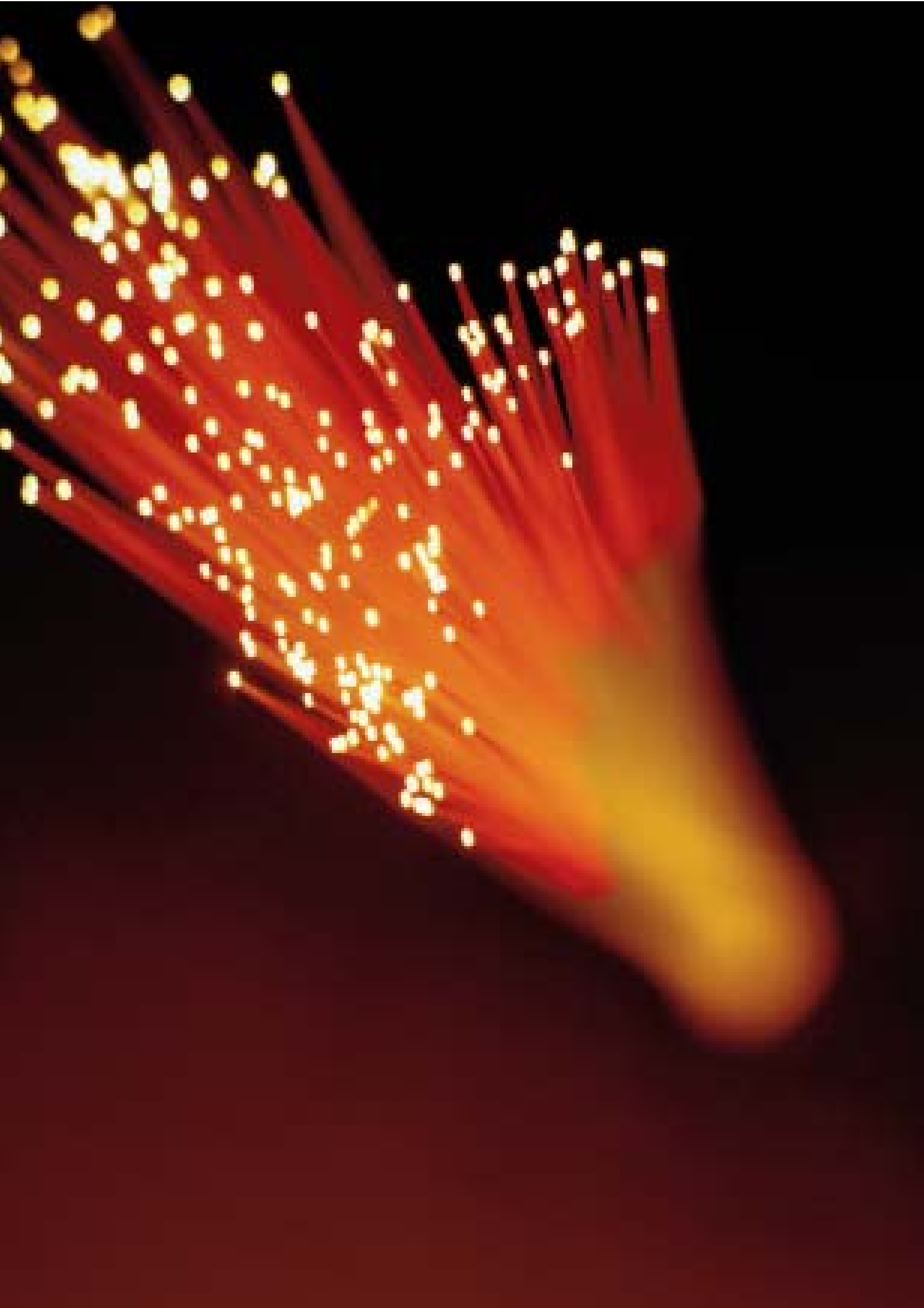
The unaccounted consequences of non-genuine software usage

ADVISORY



Table of Contents

Foreword	1
Executive Summary	3
Key Drivers	7
Potential Implications	11
Involvement of Anti-Social Elements	15
Information Disclosure and Data Theft	17
Malware Attacks	21
Extortion Using Ransomware	25
Unsecured Business Environment	29
Network Effect	31
Academic Institutions – Usage of non-genuine software by students	35
Increased Security Exposure for Government	39
Reputation Risks	43
Seeing the larger picture	45
Appendix: Methodology	51



Foreword

Explosive growth of the Internet in the last two decades has made it one of the most used channels for acquiring software quickly. At the same time, higher profit margins and minimal risks associated with counterfeiting / cracking of genuine software, have given opportunity to anti-social and anti-national elements to make non-genuine software available on the Internet as well as in the physical media. This combined with limited awareness of the implications of using such software in our user population, exposes our Information, Communication and Technology (ICT) infrastructure to various information security challenges.

The objective of this whitepaper is to sensitize readers, end users, government establishments and enterprises, to the various security implications associated with usage of non-genuine software. With this intention the paper considers the results of our research, real-life cases and hypothetical scenarios to highlight the potential information security consequences of non-genuine software usage.

The research performed during the development of this paper observed that usage of non-genuine software can now be considered a significant vector in weakening the security posture at micro and macro economic levels. The information and test cases assembled in this paper demonstrate that using non-genuine software not only increases threat of data loss and intrusions to personal systems, but also to critical ICT infrastructure of the society, thereby threatening national security. There cannot be a better time for citizens, governments and corporations to come together in the endeavor to mitigate the risks arising from the usage of these potentially dangerous systems.

Akhilesh Tuteja

Executive Director

KPMG in India



Executive Summary

It remains a well established fact that use of unlicensed or pirated software results in both immense financial implications due to infringement of the copyright laws as well as tarnishing of the company's market reputation. Studies also indicate that deployment of such software often leads to organization-wide security risks, such as loss of data privacy, system failures and downtime, and reduced operational performance. Additionally, a 2009 study carried out by KPMG indicates that non-genuine software can potentially disrupt the smooth functioning of an organization's operations by adversely affecting the system security infrastructure.

This paper seeks to establish the significant direct and indirect information security implications for government and corporate organizations as well as individuals when deploying non-genuine software. The paper elaborates the key drivers motivating the deployment of non-genuine software, the security implications thereof, and the suggested measures and considerations which government and corporate organizations can adopt for increasing awareness among users regarding security implications of deploying non-genuine software whereby reducing its usage.

Drivers

Factors such as easy availability, lower costs of acquisition, and convenience of acquiring non-genuine software as well as the attraction of deploying seemingly effective yet free software, continue to drive end users and organizations towards wide range deployment of non-genuine software.

Implications

Recent reports indicate a strong direct correlation between usage of non-genuine software and security threats such as malware and botnets.

As part of the research conducted for this white paper, we reviewed 50 websites offering non-genuine software and / or enabling tools and techniques for acquiring such software which revealed that more than 60 percent of these websites include a varying degree of threat vectors that can potentially impact information systems security.

- 60 percent websites providing cracks, keygens, warez or counterfeits have potential threat vectors
- 39 percent organizations surveyed reported security incident of non-genuine software detection in their IT environment
- 35 percent organizations cited 'ready availability' as the reason for employees to use non-genuine software
- Correlation coefficient between software piracy rates and malware attacks is a strong 0.74
- Companies using non genuine software are 43 percent more likely to have critical system failures *

*Source: Impact of unlicensed software on mid-market companies - Harrison Group

The security implications of deploying non-genuine software are multi-dimensional, including threats that directly affect the end-user and organization's security as well as indirect threats leading to increased cost of protection and remediation. Directly impacting security threats include loss of data confidentiality and integrity, as well as reduced operational performance arising from:

- Phishing Attacks
- Malware and Botnets
- Ransomware

Indirect security threats of deploying non-genuine software include the organization or user unknowingly becoming part of a larger nexus of anti-social elements funding and operating illegal pirated software businesses, thus contributing to the network of organized crime.

Given today's networked environment, where most computing devices are connected through the Internet, such threats arising from infected non-genuine software have far reaching implications for an entire network. A system having non-genuine software can adversely impact the overall security of a network. A large number of hackers develop potentially dangerous software disguised as software with rich functionalities to lure unsuspecting users. These users can then become part of Botnets and be controlled remotely for executing large scale attacks.



Measures

The paper discusses the security programs adopted by select corporations across industry sectors for discouraging use of non-genuine software and also provides recommendations for mitigating such risks.

Some of the measures that the government and industry may consider include:

- Creating awareness among end users in homes, academic institutions, public and private enterprises against the usage of non-genuine software; this includes a program specially targeted towards the student community
- Working towards effective implementation of the legal and regulatory framework to discourage deployment of infected non-genuine software
- Facilitating faster and more focused punitive action for non-compliance, including establishment of special courts
- Institutionalization of an internal program within the government and private organizations to manage and control deployment of software assets; such programs should include periodic reviews / audits of software inventory and management processes around it
- Implementing controls to prevent and detect usage of non-genuine software, especially on critical Information, Communication and Telecom (ICT) infrastructure
- Spreading the good word

At the outset ...Key Drivers

The consumer base for software in India has over the last decade witnessed an unprecedented expansion on account of a surge in PC and Internet penetration across the country. Low production costs, ease of manufacturing and high profit margins have fuelled the non-genuine software market in the country. As per the Fifth Annual Business Software Alliance (BSA) and IDC Global Software Piracy Study released in May 2008, India had a piracy rate of 69 percent in 2007.

The Internet serves to be one of the leading channels for acquiring non-genuine software. Several websites and peer to peer networks offer installable non-genuine software, product keys, key generators and crack tools. There are other equally popular channels like physical media (CDs and DVDs) that are easily available as well. As can be observed in Figure 1, irrespective of the medium used to obtain non-genuine software, the risks of getting infected with malicious software are fairly significant.

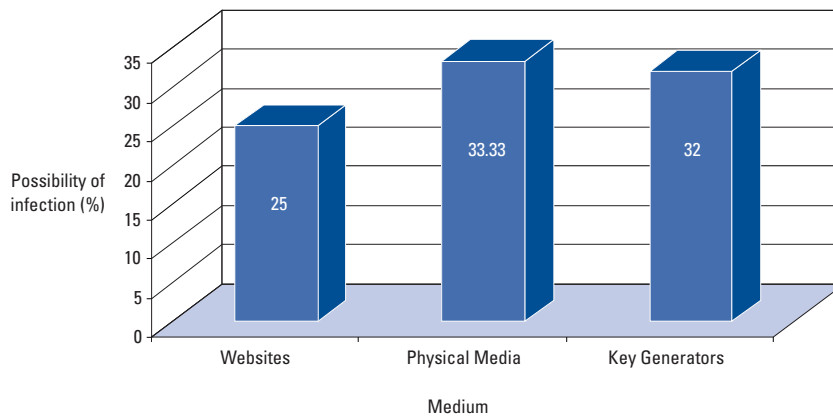


Figure 1: Possibility of infection through channel used for acquiring non-genuine software

*Source: IDC Study -The Risks of obtaining and using pirated software - 2006 and Microsoft® Internal Study: Dangers of Counterfeit Software



Information security is generally associated with terms like viruses and cyber crime. However, key information security concerns stem from various sources including:

- Discontent employees: Insider threats initiated by disgruntled employees, contractors and consultants
- Internet: Cyber crime / attacks such as botnets, exploiting browser vulnerabilities
- Mismanagement: Data breaches / loss due to mismanagement
- Terrorist attacks
- Neglected endpoints and LAN security
- Exploited vulnerabilities due to improper patch management
- Social engineering that can be assisted by social networking websites
- Malware like spyware, viruses and trojans which are usually downloaded from the Internet by unsuspecting users

The information security chain is as strong as its weakest link and end users are usually found to be this weakest link. As a user clicks on a malicious link on the Internet and downloads unauthorized software or email attachments, he / she may become a victim of social engineering attacks and sometimes knowingly or unknowingly install counterfeit / illegal or pirated software on his / her machine. With the rapid rise of the Internet and personal / mobile computing across all walks of life, the exposure of end users to these security threats has increased manifold and thus neither governments nor businesses are immune to these threats.

Our analysis suggests that users in countries with higher software piracy rates tend to be more susceptible to malware attacks (see Figure 2). The correlation coefficient between these two is a strong 0.74.

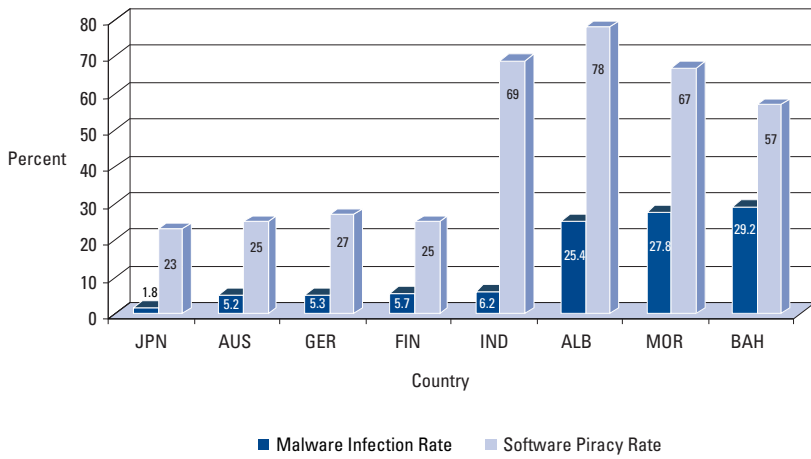


Figure 2: Malware infections are more in countries with higher software piracy

* CCM: Computers Cleaned per Mil represents the number of computers cleaned per thousand executions of the Malicious Software Removal Tool
** Malware Infection Rates as published in the Microsoft Security Intelligence Report 2008
*** Piracy rates as published in the Business Software Alliance (BSA) - 2007 Global Software Piracy Study



At the outset ... Potential Implications

In the context of individuals and businesses, increased vulnerability to malware, damage to reputation, reduced operational efficiencies and increased total cost of ownership are some of the downfalls of deploying non-genuine software. From a broader macro-economic perspective, the use of non-genuine software has the potential to adversely affect employment, tax revenues, industry growth as well as national security.

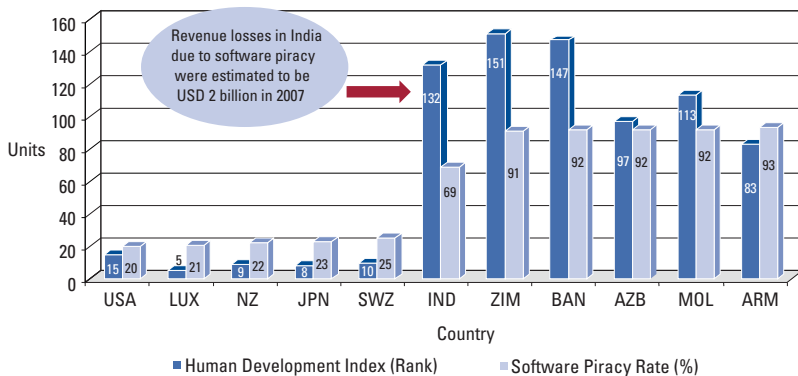


Figure 3: Software piracy trends higher in developing nations

Source: BSA - 2007 Global Software Piracy Study / United Nations HDI Rankings

As Figure 3 demonstrates, developing nations such as India still remain relatively ill equipped in dealing with software piracy. Non-genuine software exposes its users, whether they are individuals or organizations, to a plethora of information security risks. This is evident in the high correlation between non-genuine software usage and malware infections¹.

Any such security threats viz. viruses, worms, spyware and Trojans, exploit vulnerabilities in the operating system and / or the software / application installed on it. While cyber criminals are continuously on the lookout for these vulnerabilities, software developers are busy developing patches or hot fixes for plugging these vulnerabilities. It is a never ending war and the users need to continuously download these patches and hot fixes to be relatively safe in the cyber world. However, users of non-genuine software suffer a big disadvantage and are constantly vulnerable to these attacks due to the lack of patches and hot fixes being made available to them.

Every time such a user is surfing on the Internet or downloading files through emails or Peer to Peer (P2P) applications, he / she is susceptible to a plethora of

¹Correlation coefficient of 0.74 observed in Figure 2

security threats. In addition to this, users who continue to download more non-genuine software from the Internet face a double edged sword and are not only vulnerable to any new threats but are continuously exposed to more of these threats every time they visit a website providing non-genuine software or assisting in cracking (installation without license) genuine software.

Our study² of 50 websites providing various enablers for using non-genuine software viz. cracks, keygens, serials, warez, etc. reveals that there is a significantly high probability of a user browsing the Internet in search of non-genuine software to be exposed to security threats as indicated in Figure 4.

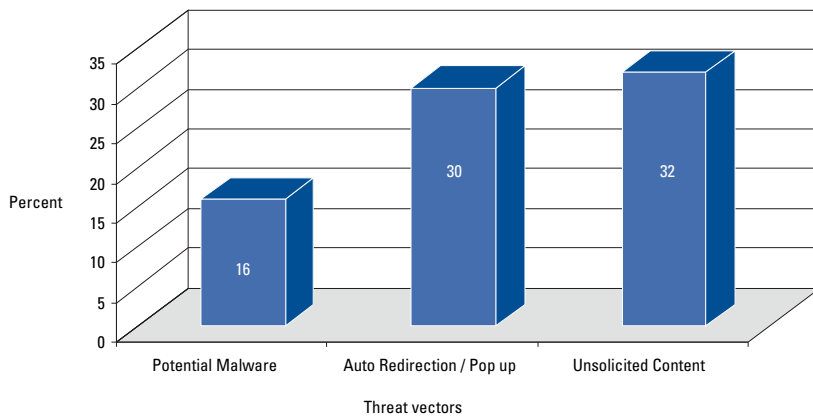


Figure 4: Threat vectors on websites providing non-genuine software

Source: An Inconvenient Reality, KPMG in India, June 2009

²KPMG study of 50 websites offering non-genuine software and/or enablers to obtain such software. Refer Annexure for methodology.

A synopsis of the potential security implications of deploying non-genuine software is outlined below.

- Involvement of Anti-Social Elements – End users of non-genuine software contribute to a chain which may potentially finance anti-social activities
- Information Disclosure and Data Theft – Users of non-genuine software could be losing valuable personal and financial data
- Malware Attacks – Hidden security and cost implications of using non-genuine software usage
- Extortion using Ransomware – Fraudsters using non-genuine software to extract money from end users
- Unsecured Business Environments – Usage of non-genuine software lowers security posture of business environments and can lead to higher critical system failures, operational downtimes and increase in the total cost of ownership in the long run
- Network Effect – Security implications of non-genuine versions of a software that is made available to masses can acquire exponential proportions due to presence of a large number of people on the networks where it is made available
- Academic Institutions and Students – Significant risks to academic institutions and students themselves due to usage of non-genuine software by students
- Increased security exposure for Government – Government sector susceptible to cyber warfare and espionage due to usage of non-genuine software
- Reputation Risks – Usage of non-genuine software can often have large financial and legal risks that may impact reputation

Information security has graduated from being a boardroom issue to an issue of national importance. The following pages attempt to demonstrate, through real life cases and hypothetical scenarios, how academic institutions, government sector organizations and unsecured business environments can become potential victims of security consequences due to the widespread use of non-genuine software.

The way forward, for end users, government and private organizations, to mitigate security risks due to usage of non-genuine software have also been discussed.



The story so far...

Involvement of Anti-Social Elements

Setting the context

Organized crime groups are often associated with illegitimate financial transactions such as money laundering. Production of non-genuine software is emerging as another means of generating revenue for anti-social elements. Since the operating costs amount to only a fraction of sales revenue, the remaining revenue often ends up in a larger resource base being used to fund counterfeit products, prostitution, weapons trading, and possibly even terrorism.

Why is software piracy such a lucrative business for organized crime groups?	
High Markups	As much as 1000 percent owing to marginal cost of production
High Demand	High demand as consumers perceive a cost advantage
Low Entry Costs	Organized crime groups use their existing infrastructure as distribution cells
Minimal Risk Level	Documented evidence on the involvement of organized crimes groups is sparse and even when implicated, the penalties levied (INR 50,000 – 2,00,000) are marginal for these large and well-resourced organizations
Victimless Crimes	Users of non-genuine software are usually aware of the product they are buying and are thus considered to be complicit in the crime

Table 1

Consider this...

In 2000, Ali Khalil Mehri, a Lebanese businessman, was arrested by Paraguayan authorities for allegedly selling millions of dollars worth of pirated and counterfeit software and funneling the proceeds to terrorist organizations³. Documents seized during the raid indicate that the sales of counterfeit goods were used for fundraising by terrorist organizations in the Middle East.

In India, there have been well documented cases of organized crime groups being involved in trade of counterfeit goods to fund their activities. The raids in 2005⁴, of large scale shipments of counterfeit goods belonging to the criminal organizations operating in India, by the US and Pakistani authorities, highlight the role played by counterfeit goods in financing the murky world of organized crime and terrorism.

Would you like to be part of a chain that potentially finances anti-social / anti-national activities or would you much rather spend that little extra and contribute to the security of our society and country?

³Middle East Intelligence Bulletin: Hezbollah's Global Finance Network: The Triple Frontier by Blanca Madani

⁴Film Piracy, Organized Crime and Terrorism"- RAND Safety and Justice Program and the Global Risk and Security Center

"In the modern world, information controls every aspect of Governance and every sector of economy. The security of ICT (Information, Communication and Technology) infrastructure, resources and data, therefore, assume high importance, priority and urgency which may even be higher than the physical security. We have a policy of periodic review of our security policy for ICT infrastructure, resources and data to mitigate risks from various threats. This is a big challenge keeping in view the size spread and capacity of the organization. Our security policy prohibits employees from using any non-genuine software owing to their high security risks. However, the software vendors should also support our cause by making the software available at affordable prices, at Purchasing Power Parity (PPP), i.e. on the basis of average earnings of a common man. This would, on the one hand, encourage the use of genuine software; on the other hand this would definitely help in discouraging use of non-genuine software in the country."

Nirmaljeet Singh Kalsi
Joint Secretary
Ministry of Home Affairs
Government of India



Information Disclosure and Data Theft

Setting the context

With rampant instances of malware in non-genuine software, data theft and disclosure of confidential information are often potential security threats. A recent report from Symantec⁵ shows that 82 percent of threats to confidential information in the Asia Pacific Japan (APJ) region were classified as threats that export user data (see Figure 5)

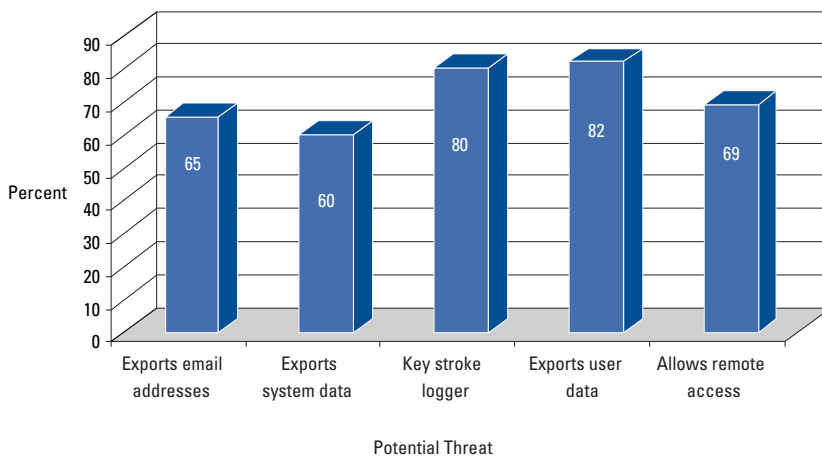


Figure 5: Threats to confidential information in the Asia Pacific Japan Region

Consider this...

Apple recently launched its iWork 09 Suite. Post the product launch; non-genuine copies were readily available on file-sharing sites. Several of the non-genuine copies, however, contained Trojan software that was bundled along with the installer package. On installation, the Trojan software connects to a remote server over the Internet and grants a remote controller access on the machine to enable malicious actions. More than 20,000 people have already reportedly downloaded the rogue installer, which was bundled with the non-genuine version of the iWorks 09 Suite.

⁵Symantec APJ Internet Security Threat Report, Trends for 2008, Volume XIV, Published April 2009



Statistics from a recent study by Scansafe⁶, as illustrated below in Figure 6, indicate that data theft Trojans as a percentage of Malware have increased significantly in 2008 (from 6 percent in 2007 to 14 percent in 2008).

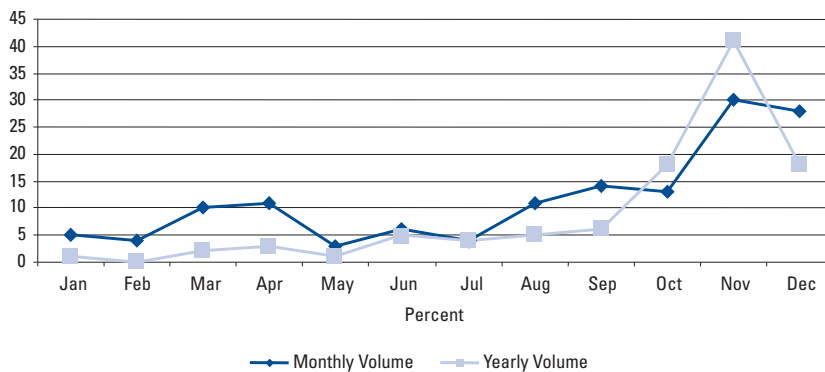


Figure 6: 2008 Block Volume – Data Theft Trojans

Other studies indicate that companies using non-genuine software are 73 percent more likely to lose confidential data and 28 percent more likely to lose a customer's personal information⁷. As a result, the risks of losing confidential data by using non-genuine software are significant for companies as well as for individuals.

When you use non-genuine software you could actually be losing valuable personal and financial data to malicious users; this could have far wider ramifications in terms of reputational, legal, financial or even business continuity risks for individuals and organizations alike.

⁶Scansafe Annual Global Report 2008

⁷Impact of the use of unlicensed software in mid market companies, White Paper by Harrison Group, 2008



Malware Attacks

Setting the context

One of the common methods of accessing / obtaining non-genuine software is through the Internet. A look at the Top 10 pirated softwares on the Internet as per the '2007 Anti-Piracy Year in Review' report released by the Software and Information Industry Association shows that several popular softwares have their non-genuine versions easily available on the Internet for a fraction of their original costs.

Rank	Software
1	McAfee VirusScan
2	Symantec Norton Anti-Virus
3	McAfee Internet Security Suite
4	Intuit TurboTax
5	Adobe Photoshop
6	Adobe Acrobat
7	Intuit Quicken Home and Business
8	Symantec Norton pcAnywhere
9	Symantec Norton Ghost
10	Adobe Creative Suite

Table 2 Top 10 pirated software on the Internet

*Source: www.siaa.net/piracy/lyir_2007.pdf

There are several websites which claim to provide access to non-genuine software through product keys, cracks and key generators. KPMG's study indicates that employees deploy non-genuine software for multiple reasons, such as easy availability of latest software versions and others as illustrated in Figure 7.

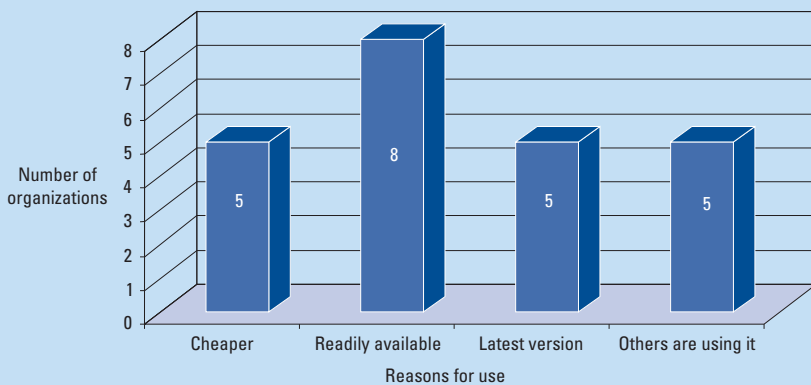


Figure 7: Reasons for employees to use non-genuine software

*Source: KPMG study



Secure Checkout

Product	Quantity	Price	Subtotal
Product 1	1	10.00	10.00
Product 2	2	15.00	30.00
Product 3	1	20.00	20.00
Product 4	3	10.00	30.00
Product 5	1	15.00	15.00
Product 6	2	10.00	20.00
Product 7	1	15.00	15.00
Product 8	1	10.00	10.00
Product 9	1	15.00	15.00
Product 10	1	10.00	10.00
Product 11	1	15.00	15.00
Product 12	1	10.00	10.00
Product 13	1	15.00	15.00
Product 14	1	10.00	10.00
Product 15	1	15.00	15.00
Product 16	1	10.00	10.00
Product 17	1	15.00	15.00
Product 18	1	10.00	10.00
Product 19	1	15.00	15.00
Product 20	1	10.00	10.00

Consider this...

A user finds a torrent⁸ on a peer-to-peer file sharing network that contains copies of Adobe software and files that appear to be key generators for the software. Unknown to the user, Malware are packaged with the torrent disguised as key generators or other executables. When the user downloads the torrent and runs such executables, the malware infects the system and typically infects system files and morphs into other seemingly useful files.

The list below highlights some of the typical actions taken by such malware while infecting a machine:

- Creates system tray popups, messages, errors and security warnings
- Makes outbound communication to other computers, phones, IM chat rooms and other services using IRC protocols
- Reads email address and phone book details
- Changes Internet Explorer (IE) options including home page, security tab, color, font, advanced menu
- Modifies the Windows Host File which could be used to stop users from visiting specific web sites by redirecting them to alternative addresses without their knowledge
- Deletes other programs
- Infects other program files to include a copy of the infection
- Hooks code into all running processes which could allow it to take control of the system or record keyboard input, mouse activity and screen contents
- Polymorphs and changes its structure
- Adds a Registry Key (RUN) to auto start programs on system start up
- Includes file creation code which is used to test for interception by security products

⁸ Torrents are files downloaded using Bit Torrents Peer-To-Peer files sharing protocol

The installed malware could be anything from a data stealing Trojan to a virus / worm or even a remotely controlled “bot”. Symantec’s recent report⁹ on Internet security threats lists India as the most affected country in the APJ region, in terms of distribution of viruses and worms (see Figure 8).

Top Countries				
Rank	Viruses	Worms	Backdoors	Trojans
1	India	India	China	China
2	China	China	India	India
3	Indonesia	Japan	Japan	Japan

Figure 8: Internet Security Threats in the APJ Region



⁹Symantec APJ Internet Security Threat Report, Trends for 2008, Volume XIV, Published April 2009

Extortion Using Ransomware

Setting the context

Several websites claim to offer genuine software and utilities at throw away prices. Fraudsters have found another innovative way of squeezing money out of the unsuspecting end user.

Consider this...

If a user wishes to obtain a copy of the Adobe Acrobat reader software, and uses the keyword 'Adobe reader' in a Google search, Google returns results with several links offering a free download of Adobe Acrobat reader software along with a sponsored link leading to a malicious / spoofed web site. Clicking on the malicious link redirects the user to a spoofed 'CNET Download.com' site which offers a free download of a copy of Adobe reader. When a user downloads and runs it, a full, operating copy of Adobe Acrobat reader is installed, but with a twist.

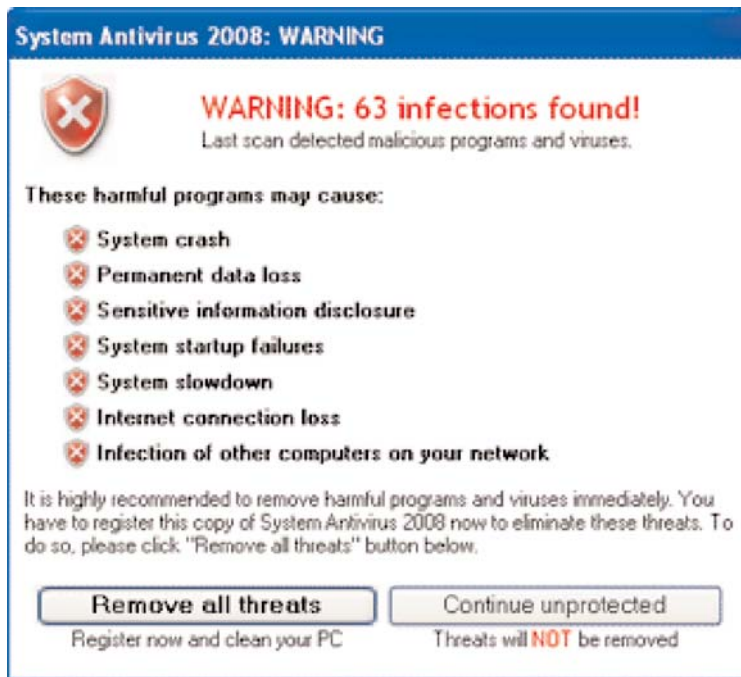


Figure 9: Ransomware message: An example

*Source: www.phirelabs.com and www.zdnet.com



After installing the program, users are interrupted with message boxes at one minute intervals. The Malware itself offers a fake remedy in the form of a pointer to a fake site which is presented as a "Remove all threats" button. After a period of time as the user tries to access files on the 'System' drive of the infected system, the ransomware starts displaying a message that the files are encrypted.

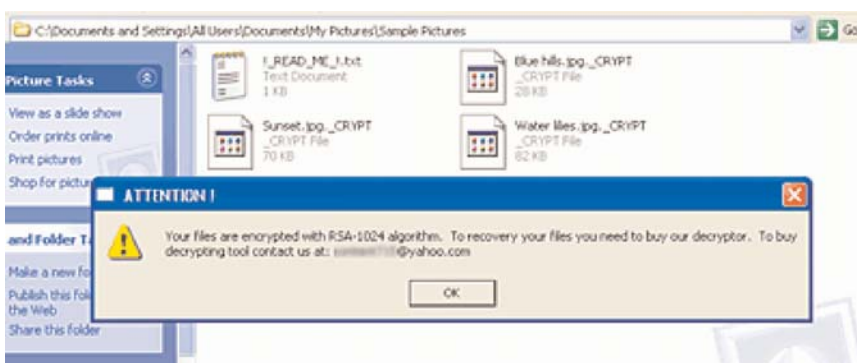


Figure 10: An example message from ransomware asking for ransom

The message clearly indicates that the victim needs to download a decryptor for decrypting data on the 'System' drive of the infected system. Accepting the message redirects the user browser to a Malware website which hosts the decryptor and which is available for download at a price.

A recent case of such ransomware was that of 'FileFix Pro', a phony utility which encrypts the user's documents and demands that the user purchase a decryptor for USD 50 for decrypting the same.

Fake anti-virus and security software is a popular target for propagators of ransomware. It is estimated that fraudsters make as much as USD 5 million through planting fake anti-virus software alone¹⁰.

Have you ever considered the possible security implications of downloading software online from an untrusted source? What could be the underlying motive for making popular software available through alternative sources that are not trusted? A question worth giving a hard thought to.

¹⁰Computerworld Security – October 31, 2008



Unsecured Business Environments

Setting the context

It is a common misconception that use of non-genuine software leads to cost reduction. Recent studies show that companies (including Small Office / Home Office (SoHo) organizations) who use non-genuine software can incur significant operational downtimes and maintenance costs, thus making the use of non-genuine software an expensive proposition in the long run.

Consider this...

As per the study 'Impact of Unlicensed Software on Mid-Market Companies' by the Harrison Group, companies using non-genuine software are 43 percent more likely to have critical system failures (some of them lasting 24 hours or more).

Apart from maintenance costs, downtime of IT systems could also translate into lost revenues, productivity and other invisible costs.

Additionally, the use of non-genuine software makes it difficult for companies to install security patches and updates, thus leaving them exposed to malware attacks. The cost of recovering from such attacks / incidents could in some cases exceed USD 1,000, thus negating the value the organization was hoping to gain through counterfeit copies of software. Thus, the cost savings of using non-genuine software are eradicated by a single security breach¹¹.

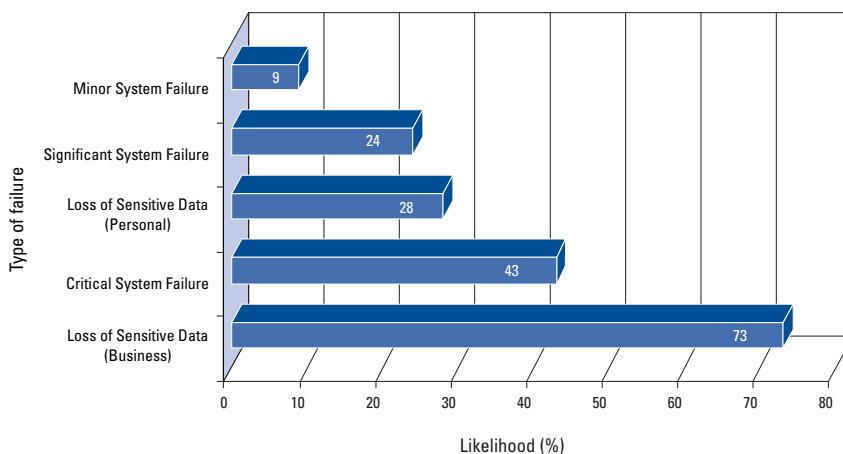


Figure 11: Likelihood of System Failure for companies using non-genuine software

*Sample Size: Original XP Users – 144, Pirated XP Users – 160

*Source: Microsoft Analysis of Risks and Issues Associated with the Usage of Pirated Software

¹¹http://www.microsoft.com/protect/promotions/us/wga_idc_us.msp

Reinforcing this is a study by Microsoft illustrated in Figure 12, which indicates that over a period of time, the total cost of ownership of pirated software is very high owing to maintenance costs and opportunity losses due to system failures and virus attacks.

For the purpose of this study, Microsoft bought and tested CDs and DVDs from various roadside vendors and carried out a survey of businesses divided between using genuine and non-genuine software.

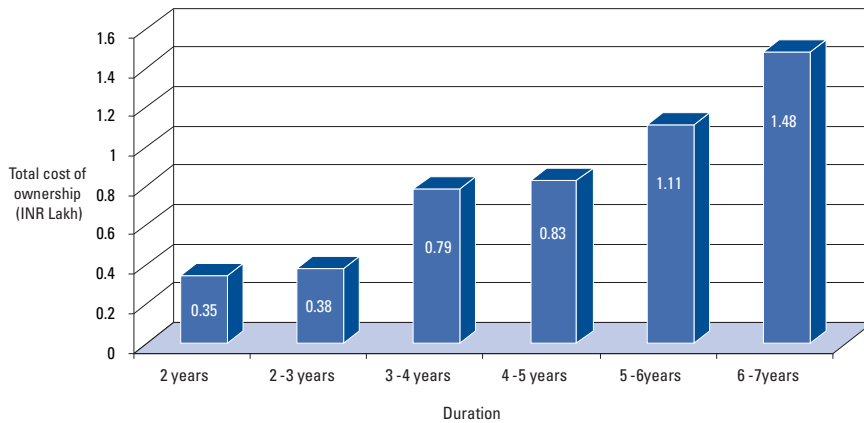


Figure 12: Increased Total Cost of Ownership

*Source: Microsoft – IDC Business Survey

Organizations may perceive that usage of non-genuine software reduces costs. However critical system failures, operational downtimes and loss of critical data, may in fact, increase the total cost of ownership in the long run.

Network Effect

Setting the context

Today, India is being recognized as the fastest growing mobile phone market in the world. According to Gartner¹², Indian cellular service revenues were USD 8.95 billion in 2006 and are projected to grow at a compound annual growth rate (CAGR) of 18.4 percent to reach USD 25.617 billion by 2011.

Consider this...

It is estimated that there are around 30 million Chinese handsets in the country which lack an International Mobile Equipment Identity (IMEI) number¹³. The IMEI is a 16-17 digit number which helps in uniquely identifying a handset and its location on the network. Currently the Cellular Operators Association of India (COAI) and the Intelligence Bureau (IB) are mulling over the security implications of a software which when uploaded to these devices would provide these devices with a unique IMEI number. As a preliminary counter measure, the Department of Telecommunications (DoT) has meanwhile instructed all service providers to disconnect these handsets from their networks.

The ramifications of an unlicensed malicious version of such a software, if created, are enormous. Even if downloaded by a small percentage of the 30 million Chinese handset users, it could lead to large scale tampering of IMEI numbers. Given the increasing role of cell phone transcripts in monitoring and investigating anti-social activities, usage of a non-genuine version of this software could lead to failure of the very objective of mitigating the risk due to presence of cell phones without IMEI numbers on the cellular networks in India.

Additionally, a malicious version of the software could also increase the risk of usage of the phone by a malicious third party as a launch pad from which worms and Trojans might launch attacks on the network.

¹²<http://www.gartner.com/it/page.jsp?id=509906>

¹³Times of India, dated 04 April 2009



As observed in Figure 13, the threat of malware in mobile devices is rapidly increasing year on year.

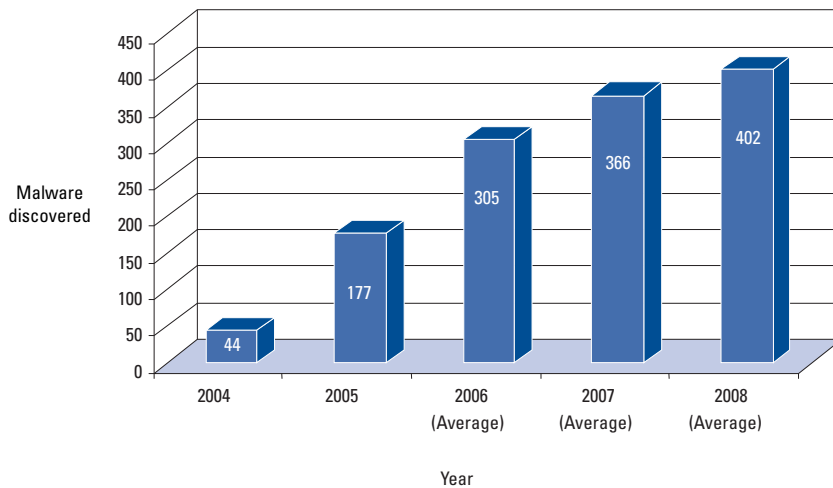


Figure 13: Growth of Mobile Malware

*Source: <http://www.cellphonehits.com>

Unlike a computer virus that can be observed and dissected on a machine that is disconnected from any network, wireless malware can spread—in some cases, even make transoceanic leaps—the moment the infected phone is powered up. It could send unwarranted MMS (Multimedia Messaging Service) and SMS (Short Message Service) messages to all contacts on the infected phone which has malicious files on it. Further, call logs of the device carrying all personal and professional contacts and data on the phone could also be sent to a commercial Internet server for viewing by a third party.

The security implications of any non-genuine software for mobile phones must be carefully understood. Imperative is to create stringent safeguards to ensure that malicious non-genuine versions of any such software are not made available.



Academic Institutions – Usage of non-genuine software by students

Setting the context

According to a study commissioned by Ipsos¹⁴ a few years ago, 61 percent of the students surveyed, never or rarely paid for commercial software programs. In addition, just under two-thirds of the college and university students surveyed, do not consider swapping or downloading digital copyrighted files (software, music and movies) without paying for them as unethical. Among students who say they would always download music or movies without paying for them, 27 percent said they regularly download and share software through a peer-to-peer (P2P) network¹⁵. Empirical studies also suggest that students tend to retain their attitudes towards usage of non-genuine software as they graduate to higher studies.

Consider this...

Students widely use P2P sharing networks such as Limewire, Morpheus and KaZaA to share files. These networks are also a popular source for sharing software, key generators and crack tools. However, unknown to the user, these files can contain malicious software in the form of Trojans and Worms which pose significant security risks. As per a study conducted by the IDC, 59 percent of the key generators and crack tools downloaded from P2P networks contained malicious or unwanted software. Another recent study¹⁶ showed that 68 percent of all downloadable responses in Limewire contained archives and executables containing malware. Some of the typical malware encountered in P2P sites like Limewire¹⁷ are listed in Table 3.

“When a user illegally downloads a movie, song, game, or software – his / her computer is likely to have been incorporated into the P2P network, possibly without the user’s knowledge. It also means that the user’s computer has very possibly been exposed to harmful viruses, worms and Trojan horses, as well as annoying pop-up advertisements. There is a real danger as well that private information on the computer has been accessible to others on the network – providing opportunities for identity thieves to obtain personal and financial information from network users who in most cases have no idea that their data is vulnerable.”

Rajiv Dalal
Managing Director
Motion Picture Dist. Association
of India (MPDA)

¹⁴“Higher Education Unlicensed Software Experience – Students and Academics Survey” , Ipsos Public Affairs – May 2005

¹⁵“Higher Education Unlicensed Software Experience – Students and Academics Survey” , Ipsos Public Affairs – May 2005

¹⁶A Study of Malware in Peer to Peer networks – Andrew Kalafut, Abhinav Acharya and Minaxi Gupta

¹⁷A Study of malware in Peer to Peer networks – Andrew Kalafut, Abhinav Acharya Minaxi Gupta




Malware Function	Definition	Typical examples	Percentage of Limewire files infected
Downloader	A computer program that is designed to download files onto a PC usually without the user's knowledge or consent. A downloader may also be programmed to perform automatic downloads in order to update itself.	Win32.Zlobdx Win32.Banload.n	45.16 percent
Worm	A virus which creates itself copies on other drives, systems or networks and performs other malicious actions which may cause systems to shut down.	Worm.Alcan.D Worm.VB.-16 Worm.P2P.Poom.A	40.32 percent
Backdoor	A Remote Control Software which allows a third-party (the attacker) to gain access and control of a victim's computer. Backdoors considered to be Trojans, can bypass security mechanisms. Backdoors are a security risk because they can gain personal information or use a victim's computer to attack a server.	NetBus BackOrifice	25.81 percent
Adware	A software program that can display advertising banners while the program is running. Adware may track a user's personal information and transfers the collected data to third parties, without the user's knowledge or consent.	Adware.ABX.Toolbar Adware.ActiveSearch Adware.Adbars Adware.AdBlaster	4.84 percent
Dialer	Dialer is a computer program used to redirect user's telephone connection to the more expensive line with higher charges for a content provided with or without a user's consent.	Adware.Adhelper Dialer.Antispy Dialer.Asdplug Dialer.AxFreeAccess	4.84 percent
Keylogger	A malware that cuts off the data exchange between the user entering it and the intended recipient application. It records any information that the user types at anytime using his / her keyboard and can send it to a third party. Keylogger creates the log file which can be sent to a specified receiver. Trojan and Pup keyloggers are functionally identical.	Keylogger.Cone.Trojan Keylogger.Mose Keylogger.Stawink	3.23 percent

Table 3

The table suggests that files and unlicensed software obtained by students through P2P networks pose significant information security risks to educational institutions.

The risks could also often be regulatory non-compliance. A case in point is where the Software and Information Industry Association (SIIA)¹⁸ was involved in an investigation of a university in the mid-west region (USA) where the students were creating Warez¹⁹ sites / content on college servers.



Whilst, some educational institutions in India have documented policies in place to discourage usage of non-genuine software, the extent of their effectiveness in serving as a deterrent to students is debatable. Effective student awareness programs, counseling and appropriate disciplinary actions would go a long way in curbing the rampant usage of non-genuine software by the student community.

¹⁸ What is Piracy-The Piracy problem (SIIA)

¹⁹ "Warez" refers to copyrighted works traded in violation of copyright laws

Increased Security Exposure for Government

Setting the context

Studies²⁰ show that the IT spend by the Indian public sector is one of the fastest growing amongst Asian countries. Within the public sector, a significant percentage of IT spend is done by the defense, internal security agencies (such as the intelligence, immigration) and public safety agencies.

Typically government departments / organizations are the ones who are involved in large turnkey IT outsourcing contracts where the scoping of the deployment of genuine software is seen to remain unclear amongst outsourcing organization, service provider and software vendor. It has been seen that this increases security exposure during large deployments or projects in government enterprises.

Consider this...

A government department decides to upgrade their existing IT infrastructure / network and invests in substantial new IT hardware. Whilst original operating systems are purchased for key servers, unlicensed software is installed on a few end user systems. Unknown to the users, the unlicensed software consists of a backdoor, which allows the host to be remotely controlled by a command-and-control server. Subsequently, sensitive files are accessed and relayed to the controllers through encrypted schemes that provide cover and stealth from existing intrusion prevention mechanisms.

²⁰ Such as the study conducted by 'Springboard Research', a Singapore based firm in 2006





A recent investigation conducted by Information Warfare Monitor²¹ shows that the above scenario is not far fetched from reality. The investigation revealed the existence of a global malware based cyber espionage network (termed as the GhostNet) which compromised at least 1295 computers in 103 countries, including 53 IP addresses in India. A large percentage of the targets were located in government institutions such as embassies and ministries of foreign affairs, including several Indian embassies, as illustrated in Table 4.

Organization	Confidence	Location	Infections
National Informatics Center, India	L	IN	12
Software Technology Parks of India	L	IN	2
Office of the Dalai Lama, India	H	IN	2
Tibetan Government in Exile, India	H	IN, US	4
Embassy of India, Belguim	L	BE	1
Embassy of India, Serbia	L	CS	1
Embassy of India, Germany	H	DE	1
Embassy of India, Italy	H	IT	1
Embassy of India, Kuwait	H	KW	1
Embassy of India, USA	H	US	7
Embassy of India, Zimbabwe	H	ZA	1
High Commission of India, Cyprus	H	CY	1
High Commission of India, United Kingdom	H	GB	1

Table 4: Government of India institutions affected by GhostNet

*Source: Tracking GhostNet – Investigating a Cyber Espionage Network, Information Warfare Monitor (IWM), Canada, March 2009

"Government departments cannot use, or condone the use of, unauthorized software. The consequence of usage of non-genuine software in our department could be serious from a security perspective. The risk of compromise of our databases not only impacts the reputation of the department and the ministry, but also is a kind of ransomware that could be used by malicious elements of the society to track financial positions of citizens and hold them for ransom."

Neeraj Kumar
 Joint Director of Income Tax
 Directorate of Income-Tax (Systems)

²¹Tracking GhostNet – Investigating a Cyber Espionage Network, Information Warfare Monitor (IWM), Canada, March 2009

Increasing adoption of Internet enabled technology solutions combined with the high software piracy rates in India could be a contributing factor in making the government sector more susceptible to attacks such as the botnet attacks described above. As seen in the Figure 14, several botnet attacks can be traced to countries such as China, Brazil, South Korea and Poland where there is a medium - high software piracy rate.

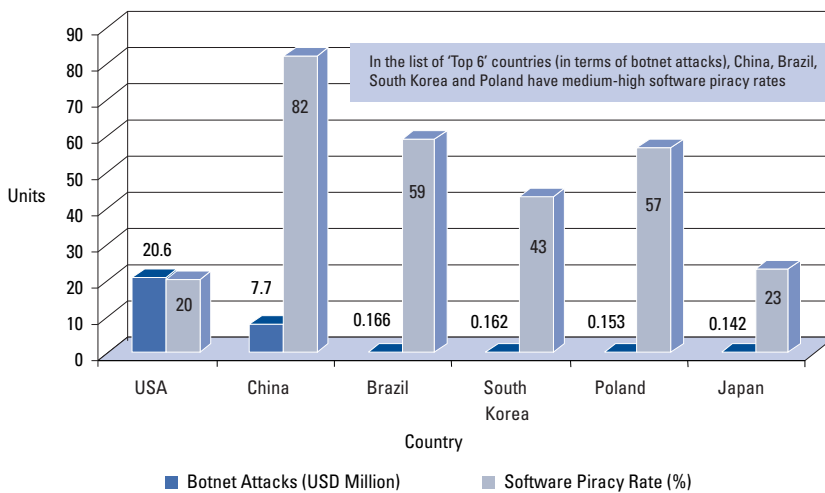


Figure 14: Correlation between software piracy and botnet attacks

*Source: Business Software Alliance (BSA) - 2007 Global Software Piracy Study, www.Securityfocus.com

As countries jostle for supremacy over the strategic cyber domain, the threat of cyber espionage is an existing reality. Installation of non-genuine / unlicensed software on any IT systems in government offices may result in irretrievable losses of strategic information to hostile third parties.

Reputation Risks

Setting the context

The government can criminally prosecute an organization for copyright infringement and if convicted, fines can range from INR 50,000 - 2,00,000 and a minimum jail sentence of 7 days going upto 3 years can be levied as well²². According to the BSA²³, in 2008, non-genuine software cost businesses in the UK as much as £16 million in legal fines. Last year, the BSA took 294 legal actions on behalf of its members in the UK and more than 3,000 legal actions were conducted across Europe and Africa.

Consider this...

In March 2009, BSA reported to have settled claims of USD 350,909 from four California-based companies for having unlicensed copies of software installed on their computers. The companies paid damages in the range of USD 70,000 to USD 110,000 for having unlicensed copies of software such as Adobe, Symantec and Microsoft software installed on its computers. As part of the individual settlements, the companies have agreed to delete all unlicensed copies of software installed on their computers, acquire any licenses necessary to become compliant, and commit to implementing stronger software license management practices.

Wouldn't you rather be involved with improving business efficiencies and productivity instead of wasting time and resources in settling legal suits and re-establishing reputation?

²²Indian Copyright Act & <http://www.nasscom.in/Nasscom/templates/NormalPage.aspx?id=6250>

²³<http://www.itpro.co.uk/index.php/609881/pirated-software-costs-firms-16-million>



The way forward

Seeing the larger picture ...

The intent of this white paper has been to highlight the far reaching impacts of using non-genuine software on the security of individuals, businesses, governments and nations. In the discussions above, we have attempted to bring to the forefront the evident as well as the concealed implications that non-genuine software usage has on its stakeholders.

The surge in Internet penetration, which provides easier access to non-genuine content available online, coupled with nascent compliance infrastructure, low end user awareness levels and weak legal enforcement, pose a formidable challenge in combating non-genuine software usage.

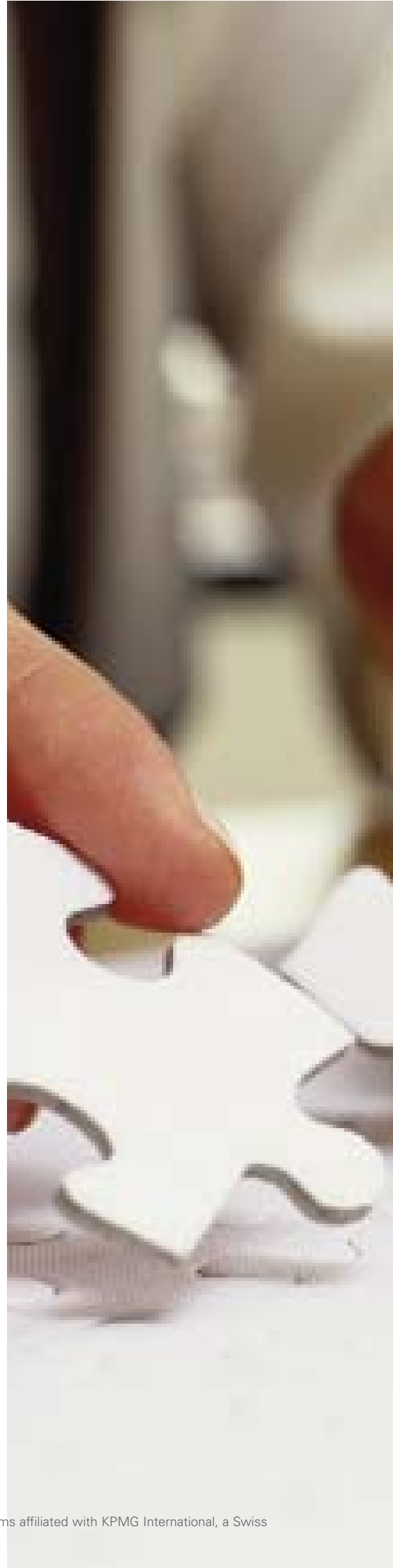
The Indian government has taken cognizance of the various information security threats and has set up CERT-IN (Computer Emergency Response Team - India) with the charter to become the nation's most trusted referral agency of the Indian community for responding to computer security incidents as and when they occur; the key objective being to reduce the risks of computer security incidents²⁴.

In addition to the services provided by CERT-IN, the Government of India's Central Vigilance Commission (CVC) has issued guidelines to control the menace of counterfeit IT products including operating systems²⁵. India's new IT Act that was recently passed by the parliament also changes the country's approach to user generated content and piracy of copyright content on the web and mobile.

Many businesses today have created special roles in the ranks of Chief Security officers (CSO) / Chief Information Security Officers (CISO) to limit the hazards of information security threats. Appropriate mindshare on issues like weak security controls, inadequate security organizations, non-genuine software usage, low levels of security awareness and management commitment towards the information security program, help provide reasonable assurance that these threats are minimized and managed well.

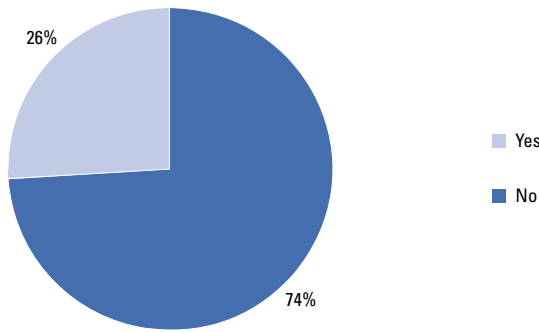
²⁴Source : <http://www.cert-in.org.in/mission.htm>

²⁵Source: <http://www.cvc.nic.in/007crd008.pdf>

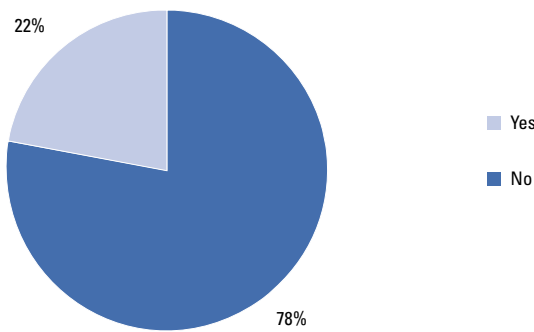




Organizations are taking initiatives for conducting security awareness sessions to make the employees aware of the numerous threats and, enable them to take proactive measures to safeguard themselves and their organizations from becoming victims of the various information security threats. In a survey conducted by KPMG²⁶, majority of CIOs / CISOs stated that their organization had an employee awareness program on security implications of using non-genuine software and that they were well aware of industry initiatives and government regulations around it (Figure 15).



Employee awareness program on security implications of non-genuine software



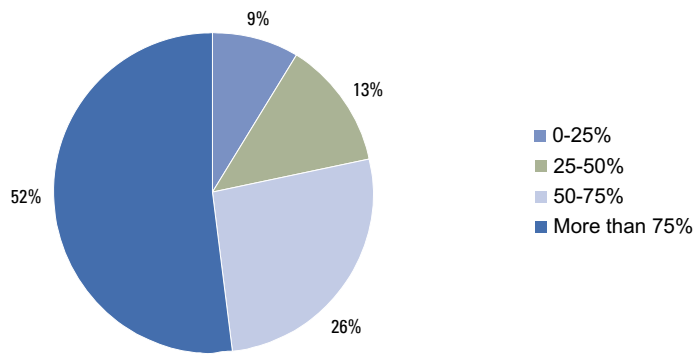
Aware of measures taken by industry / government to combat usage of non-genuine software

Figure 15

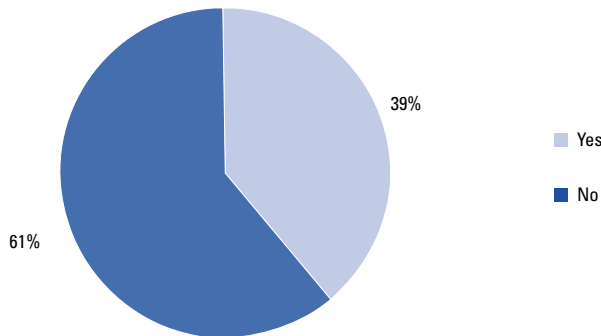
*Source: KPMG study

²⁶ KPMG survey of CIO/CISOs, 'An Inconvenient Reality, KPMG in India, June 2009'

Our survey indicates that the percentage of organizations stating that, significant number of its employees are aware about security implications of using non-genuine software, is high. Further, the number of organizations where security incidents are being reported for identification / detection of non-genuine software is also fairly high (Figure 16).



Percentage of employees aware of security implications of using non-genuine software



Any security incident reported on identification of non-genuine software in organizations

Figure 16

*Source: KPMG study

The above analysis indicates that while some of the corporate consumers are aware of the risks of using non-genuine software and are taking initiatives to discourage it, there still exists a large section of user groups – small office and home users - that are ignorant of the potential consequences.

Organizations should institute a program for discouraging use of non-genuine software

- Create a formal list containing program name, copies available, serial numbers, version numbers and future upgrade requirements
- Run awareness training programs for employee and communicate organization's commitment to genuine software
- Obtain undertaking from all third parties to ensure they only supply and use genuine software
- Ensure controls are enforced to prevent and detect installation of non-genuine software
- Ensure compliance by periodic audits

As end users continue to perceive a cost advantage in using non-genuine software, there is an imminent need for the industry, academic institutions and the government to play an active role in creating awareness on the risks of software piracy. Public education campaigns and awareness directives should be used as a medium to help users make informed choices with respect to purchase of software. Educational institutions should implement effective software asset management policies to regulate the use of non-genuine software in their facilities.

Users need to be more aware

- Buy software from genuine sources
- Check online for authenticity of the serial numbers on the suppliers genuine online website
- Validate for genuine identification marks on the installation media / packaging
- Assess the genuine identification marks on the websites, prior to downloading, to distinguish between genuine and fake websites providing downloads
- Preserve all original licenses and documents
- Adhere to policies on usage of genuine software in the workplace

The existing legal and regulatory frameworks also need to be strengthened and rigorously enforced to dissuade individuals and corporations from being a part of the non-genuine software chain. Existing government initiatives such as the appointment of the Copyright Enforcement Advisory Council (CEAC) and creation of piracy targeting cells in State Police Headquarters should be expanded and strengthened both in scope and operations.

Considerations for the Government

- Development and roll out of a program for sensitizing students and parents alike on the security impacts of using non-genuine software
- Facilitate faster and more focused punitive action for non-compliance; set up of special courts dealing specifically with Intellectual Property issues may be considered
- Obtain undertaking from all third parties to ensure they only supply and use genuine software
- Ensure controls are enforced to prevent and detect installation of non-genuine software
- Ensure compliance by periodic audits

Only a concerted effort from the industry, the government and the consumers can possibly ensure minimization of information security risks arising from usage of non-genuine software.

Appendix: Methodology

The methodology deployed in the development of this whitepaper was primarily a combination of limited primary research, assorted discussions with government and corporate representatives and secondary research.

We performed a study of 50 select websites providing counterfeit software and / or various enablers to non-genuine software (such as cracks, key generators, serials and warez), with the objective of identifying threat vectors like potential malware, auto-redirections / pop-ups, and unsolicited content. The approach adopted was to visit the home page and the page for one sample download.

In addition, we performed a survey of a group of Chief Information Officers / Chief Information Security Officers (CIO / CISO) of organizations to understand their views on programs for, and awareness of security implications of using non-genuine software. This survey was performed using a survey questionnaire focusing on identification of:

- Existence of employee awareness program on security implications of using non-genuine software
- Proportion of employees aware about security implications of using non-genuine software
- Any security incident reported on usage of non-genuine software
- Reasons for an average employee to use non-genuine software
- Awareness about measures taken by government / industry to combat usage of non-genuine software

The secondary research information sources include:

- Business Software Alliance (BSA) – 2007 Global Software Piracy Study
- Scansafe Annual Global Report 2008
- Harrison Group Whitepaper on Impact of the use of unlicensed software in mid-market companies (2008)
- Tracking GhostNet – Investigating a Cyber Espionage Network, Information Warfare Monitor (IWM), Canada, 2009
- IDC whitepaper on Risks of Pirated Software
- Symantec APJ Internet Security Threat Report, Trends for 2008, Volume XIV, Published April 2009



KPMG in India

Mumbai

KPMG House, Kamala Mills Compound
448, Senapati Bapat Marg,
Lower Parel,
Mumbai 400 013
Tel: +91 22 3989 6000
Fax: +91 22 3983 6000

Delhi

DLF Building No. 10,
8th Floor, Tower B,
DLF Cyber City, Phase 2, Gurgaon 122 002
Tel: +91 124 307 4000
Fax: +91 124 254 9101

Bangalore

Solitaire
139/26, 3rd Floor,
Inner Ring Road, Koramangala,
Bangalore 560 071
Tel: +91 80 3980 6000
Fax: +91 80 3980 6999

Chennai

No.10 Mahatma Gandhi Road
Nungambakkam
Chennai 600 034
Tel: +91 44 3914 5000
Fax: +91 44 3914 5999

Hyderabad

8-2-618/2
Reliance Humsafar, 4th Floor
Road No.11, Banjara Hills
Hyderabad - 500 034
Tel: +91 40 6630 5000
Fax: +91 40 6630 5299

Kolkata

Park Plaza, Block F, 6th Floor
71 Park Street
Kolkata 700 016
Tel: +91 33 4403 4000
Fax: +91 33 4403 4199

Pune

703, Godrej Castlemaine
Bund Garden
Pune 411 001
Tel: +91 20 3058 5764/65
Fax: +91 20 3058 5775

KPMG Contacts

Pradip Kanakia

Head of Markets
Tel: +91 (80) 3980 6100
e-Mail: pkanakia@kpmg.com

Akhilesh Tuteja

Executive Director
Tel: +91 (124) 3074800
e-Mail: atuteja@kpmg.com