



## Pressing need to review legal and regulatory framework to tackle non-genuine software issues

### *Security implications of deploying non-genuine software are multi-dimensional*

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

**August 26, 2009** : Non-genuine software can potentially disrupt the smooth functioning of an organizations' operations by adversely affecting the system security infrastructure; indicates a recent study conducted by KPMG. The study titled "An Inconvenient Reality—The unaccounted consequences of non-genuine software usage" 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.

As part of the research conducted for the report, KPMG reviewed 50 websites offering non-genuine software and/or enablers for non-genuine software usage, like key generators. The study revealed that more than 60 percent of these websites include a varying degree of threat vectors that can potentially impact information systems security.

Speaking on the release of this report, **Mr. Akhilesh Tuteja, Executive Director, IT Advisory Services, KPMG in India** said “Explosive growth of the Internet in the last two decades has made it one of the most used channels for acquiring software quickly and 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.” He added “The objective of this whitepaper is to sensitise 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.”

### **Threat to National Security**

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 Information, Communication and Telecom infrastructure of the society thereby threatening national security.

The report tells that one of the most common methods of accessing non genuine software is through the Internet. The 2007 Anti Piracy Year in Review report from Software and Information Industry Association shows that several popular software have their non genuine versions easily available on the Internet for a fraction of their original costs. KPMG's study indicates that employees deploy non-genuine software for multiple reasons, such as easy availability of latest software versions, cheaper rates and latest versions.

### **Potential Risks**

A system having non-genuine software can adversely impact the overall security of a network. A large numbers 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. Large numbers of students never or rarely pay for commercial software programs. According to Ipsos Public Affairs study in the US, this number is put at 61% globally and of which 27% use Peer to Peer (P2P) networking for downloading non-genuine software. Another recent study by IDC, indicates that 59% of key generators and crack tools downloaded from such P2P sites contain malware. This indicates the vulnerability of the student community in the country & globally to the security risks of using non-genuine software.

### **Some security measures**

The report 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

---

**About KPMG:**

KPMG is the global network of professional services firms of KPMG International. KPMG member firms provide audit, tax and advisory services through industry focused, talented professionals, who deliver value for the benefit of their clients and communities.

KPMG in India has offices in Mumbai, Delhi, Bangalore, Chennai, Hyderabad, Kolkata Pune and Kochi.

Log on to [www.in.kpmg.com](http://www.in.kpmg.com) for a copy on the report

---

**For further information contact:**

Subir Moitra Senior Manager – Marketing & Communications KPMG - Delhi Mobile : +91 98111 99613 e-Mail : smoitra@kpmg.com	Archana Dabral Senior Manager – Marketing & Communications KPMG – Mumbai Mobile: +91 982000 4441 e-Mail : archanadabral@kpmg.com
--	--

-ENDS -