Survey finds that unlicensed software is still a threat

Fewer South African companies are using unlicensed software, opting to avoid the numerous security threats associated with counterfeit software, but one in three copies of software installed on local PCs during 2013 was still not properly licensed. The estimated commercial value (locally) of the unlicensed software is R4.11 billion.

Image: www.freedigitalphotos.net

This, according to the latest BSA Global Software Survey, which states that there has been a one percentage-point decrease in the use of unlicensed software since 2011. The survey is conducted every second year by market research firm IDC and this year polled PC users in 34 markets including nearly 22,000 consumer and business users and more than 2000 IT managers. BSA¦The Software Alliance is a non-profit trade association established to advance the goals of the software industry and its hardware partners. The organisation also represents Adobe, Autodesk and Noctranet, and Symantec in South Africa.

"Hopefully this drop signals the start of a downward trend," said Marius Haman, chairman of the South Africa committee of BSA¦The Software Alliance and corporate attorney in the Digital Crimes Unit, Legal & Corporate Affairs of Microsoft Middle East & Africa. "Compared to unlicensed products, properly licensed software offers computer users more peace of mind when it comes to operational efficiency and security. Corporate users and general PC users are starting to view this peace of mind as an important component of success in business."

Being hacked or having your data stolen

The biggest deterrent to using unlicensed software is being hacked or having your data stolen, as 64% of global computer users cited unauthorised access by hackers as a top threat while 59% of respondents cited loss of data.

This paranoia over malicious software being added into pirated software is not unfounded as the risks of using unlicensed software goes beyond breaking the law and infringing intellectual property rights of software vendors.

In a research white paper entitled The Dangerous World of Counterfeit and Pirated Software, IDC found that 78% of unlicensed software downloads included some form of tracking cookie or spyware installations. These install themselves on a user's PC and report personal information without the user's knowledge, such as credit card data, passwords and email contact lists, which can all be exploited by cybercriminals.

When it comes to Trojans and other malicious adware, 27% of the downloaded counterfeit software incorporated them, which at best threaten a computer's performance and may even cause it to crash, leading to costs in terms of data and productivity losses. In the worst-case scenario, the malicious software may also perform actions that are not authorised by the PC user, like data deletion or copying of corporate information.

Often, malicious software also prevents the installation of patches that Microsoft and other software vendors send to fix any vulnerability that hackers exploit, causing PCs to remain vulnerable.

In spite of the potential damage that unlicensed software might cause to PC systems and networks, fewer than half of IT managers are very confident that their company's software is properly licensed. Moreover, only 35% of businesses worldwide have written policies put in place that expressly require the use of properly licensed software.

Only purchase software from reputable companies

"Businesses should ensure that they only purchase software from reputable companies, as a seller proposing to violate copyright law could just as easily view your credit card data or personal information as another source of revenue that can be sold to identity thieves," warned Dale Waterman, who leads the Microsoft Digital Crimes Unit in the Middle East and Africa region.

Waterman added that the use of unlicensed software can easily be deterred within the business environment through the establishment of a formal policy on licensed software use. South African organisations have to consider implementing more robust software asset-management programs that ensure adequate controls are in place to provide a full view into what is installed on a network, and help to avoid the occurrence of security and operational risks.