

ByteShield™ Proposes that Anti-piracy Efforts need Better Technology, Not only Better, Bigger Legal Teams

San Francisco, CA, June 17, 2008 - ByteShield Inc., a leading provider of user and developer friendly software usage control, proposes that the software industry, in addition to its successful legal efforts, needs a new and effective technology approach to software usage control, IP protection and anti-piracy.

The May 14, 2008 report issued by the Business Software Alliance (BSA) and IDC (<http://global.bsa.org/idcglobalstudy2007/>) shows the worldwide PC software piracy rate increased in 2007 by 3% (to 38%) and software company losses increased by 20% (to \$48B).

ByteShield contends that while the problem could have been much worse without the BSA's many, diverse and successful legal actions to suppress software piracy, the evidence clearly shows that additional approaches are necessary because the problem continues to exist and grow.

"We congratulate the BSA on its good work and progress over many years but the industry is still losing ground on this issue," said Jan Samzelius, CEO of ByteShield. "To really address this issue, the software industry companies need to realize that the legal approach alone, as good as it is, is not sufficient to do the trick - the incentives are too high and the risk of getting caught is simply too low. In addition to the legal action, the industry needs to drive user friendly technology solutions and education - perhaps via another organization or via broadening the BSA's role."

The 3 pre-requisites for software piracy (and any other technology proliferation) are:

1. Existence and access to cracking technology
2. Knowledge and skills to apply this technology
3. Willingness to apply it.

Once a technology (anything from nuclear bombs to software piracy) exists, the first two prerequisites move from mega-R&D costs to affordable cost (for rogue states or individuals) - so a legal-only approach constrains only the 3rd prerequisite. In the case of software piracy - debuggers, disassemblers, decompilers (to name a few 'tools of the cracking trade'), and the skills to use them for evil have proliferated. Through the BSA, the software industry has tried to ensure legal constraints but the problem continues to grow. So what should the industry do?

Admitting self-interest, ByteShield's technological approach to protecting software acknowledges that any protection created by man can eventually be cracked by man. In comparison to conventional software protection technologies usually based on a single hurdle, ByteShield has multiple hurdles where one removes small but critical pieces of the code it protects and then replaces them at run-time. A cracker may find and 'fix' one piece in a certain amount of time, but if 1,000, 10,000 or even 100,000 pieces of code need to be 'fixed', one by one, then the effort required is too great. Beyond that approach ByteShield™ recognizes that 'effective software usage control' must have no tangible impact on honest users. Only ByteShield's new approach, incorporating a remote license server, delivers user-friendly features such as permitting multiple installations, multiple activations and easily movable activations and has no impact on development teams - the protection is applied post-development.

About ByteShield

ByteShield is the first affordable, software-based, strong solution that actually works and is user and developer friendly. Once usage is controlled, various new business models can enable additional revenue generation (e.g. rental, subscription, SaaS). ByteShield, which is a privately held California corporation, was established in September, 2004 with headquarters in San Francisco, California. To find out more, visit www.ByteShield.net or call +1 415 420 6636.

All brand names, product names, or trademarks belong to their respective holders