

Take Steps to Combat Digital Piracy in Your Enterprise

David Mitchell Smith, L. Frank Kenney

A government crackdown on piracy should spur enterprises to comply with the law before federal agents arrive. Some enterprises unknowingly use illegal copies of software, but they are still legally liable.

NEWS ANALYSIS

Event

On 11 December 2001, U.S. Attorney General John Ashcroft announced that separate undercover probes into pirated software and Internet content had led to some 100 search warrants against organizations that illegally copy software, digital music and games, and movies. Federal agents have targeted students, employees of technology firms, executives and government workers who comprise an underground group known as Warez, which altered original software code to thwart antipiracy techniques.

Analysis

With Internet piracy rampant, the United States has for more than a year conducted investigations to expose sources of piracy of intellectual property. The discovery of Warez (and other groups such as Appz, Crackz and Mp3) will accompany searches at universities and at companies where insiders steal products for illegal duplication. To combat piracy effectively, law enforcement agencies must attack the three segments that comprise the underground piracy apparatus:

- **Tier 1:** large organizations that pirate software, movies and music for profit. They may employ hundreds of persons and use sophisticated technology to duplicate and distribute millions of copies of pirated goods. They often operate where local governments ignore their activities (e.g., China, India, Indonesia and South Korea).
- **Tier 2:** large organizations that pirate for recognition from peers, not profits. They rely on the Internet — e.g., the Internet Relay Chat network — to plan, promote and distribute pirated goods. Their diverse membership includes students, IT professionals and business executives.
- **Tier 3:** individuals who ignore license agreements and pirate for individual use or for sharing among friends or family. They often copy music and games for use on PCs.

Gartner warns enterprises to pay special attention to the potential for Tier 2 piracy occurring in their organizations or for the fruits of such piracy being used there. Businesses are legally liable for what their employees do on company premises. Therefore, the execution of a search warrant or other investigative activities may disrupt or shut down enterprise operations. Authorities and enterprises should also target each tier individually. Focusing on understanding the composition, methods and motives of Tier 2 pirates, however, will likely do the most to dismantle Warez and other pirate groups.

Analytical Sources: David Smith, Internet Strategies, and Frank Kenney, Information Security Strategies

Need to Know: Reference Material and Recommended Reading

- "Protect Your Intellectual Assets With These Seven Steps" (FT-15-1149) Enterprises should implement mechanisms to protect their intellectual property. Gartner provides seven recommendations to do so. **By Colleen Young**
- "Secure File Transfer: Tactical and Strategic Solutions" (T-15-0165) The common file transfer protocol (ftp) process carries security risks that need plugging via suitable third-party solutions. **By Frank Kenney, Vic Wheatman and Richard Stienon**

(You may need to sign in or be a Gartner client to access all of this content.)

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509