

High-Profile Thefts Show Insiders Do the Most Damage

John Pescatore

Two recent cases show that insiders – not outside cyberattacks – are responsible for most incidents that cause real losses. Enterprises must find ways to ensure security while still allowing appropriate information access.

Event

On 25 November 2002, New York City authorities charged three people in an identity theft scheme that allegedly victimized more than 30,000 people and resulted in the theft of at least \$2.7 million. A low-level employee of a software company who had illegal access to credit histories allegedly made the theft possible. The charges follow the 12 November 2002 arrests of three persons — including an employee of an online betting company — who allegedly rigged betting on the Breeders' Cup horse race to obtain a fraudulent payout of \$3 million.

Analysis

Gartner estimates that 70 percent of security incidents that actually cause loss to enterprises — rather than mere annoyance — involve insiders. This finding should surprise no one. Insiders create an enterprise's products and deliver its services, and efficient access to sensitive information is essential to its efforts to bring profitable products to market quickly and competitively. Nonetheless, enterprises must find the balance between completely open internal access and overprotective security that hurts business. Enterprises can achieve this balance by:

- **Conducting background investigations before employees are hired.** Background investigations should be required for all employees — including system and security administrators — who will have access to sensitive information.
- **Enforcing "need to know" policies.** Consolidated access management architectures should be deployed to allow server and database access only to employees who require it for legitimate business purposes. Audit and reporting tools should be used to review privilege escalation actions.
- **Using acceptable-use enforcement technology.** Enterprises should "trust but verify" by using tools from providers such as Nixsun, SilentRunner and Vericept and that enable them to spot policy violations or illegitimate access to sensitive information within vast amounts of internal traffic.

Analytical Source: John Pescatore, Gartner Research

Recommended Reading and Related Research

- "Fixing the FBI's 'Top 20' Security Flaws Isn't Enough" — The FBI provides a solid IT security framework, but enterprises must go beyond its recommendations. **By John Pescatore**
- "Internet Filtering and Reporting: Websense vs. SurfControl" — Software tools enable enterprises to block inappropriate Internet sites and report on usage. **By Bill Gassman**

(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