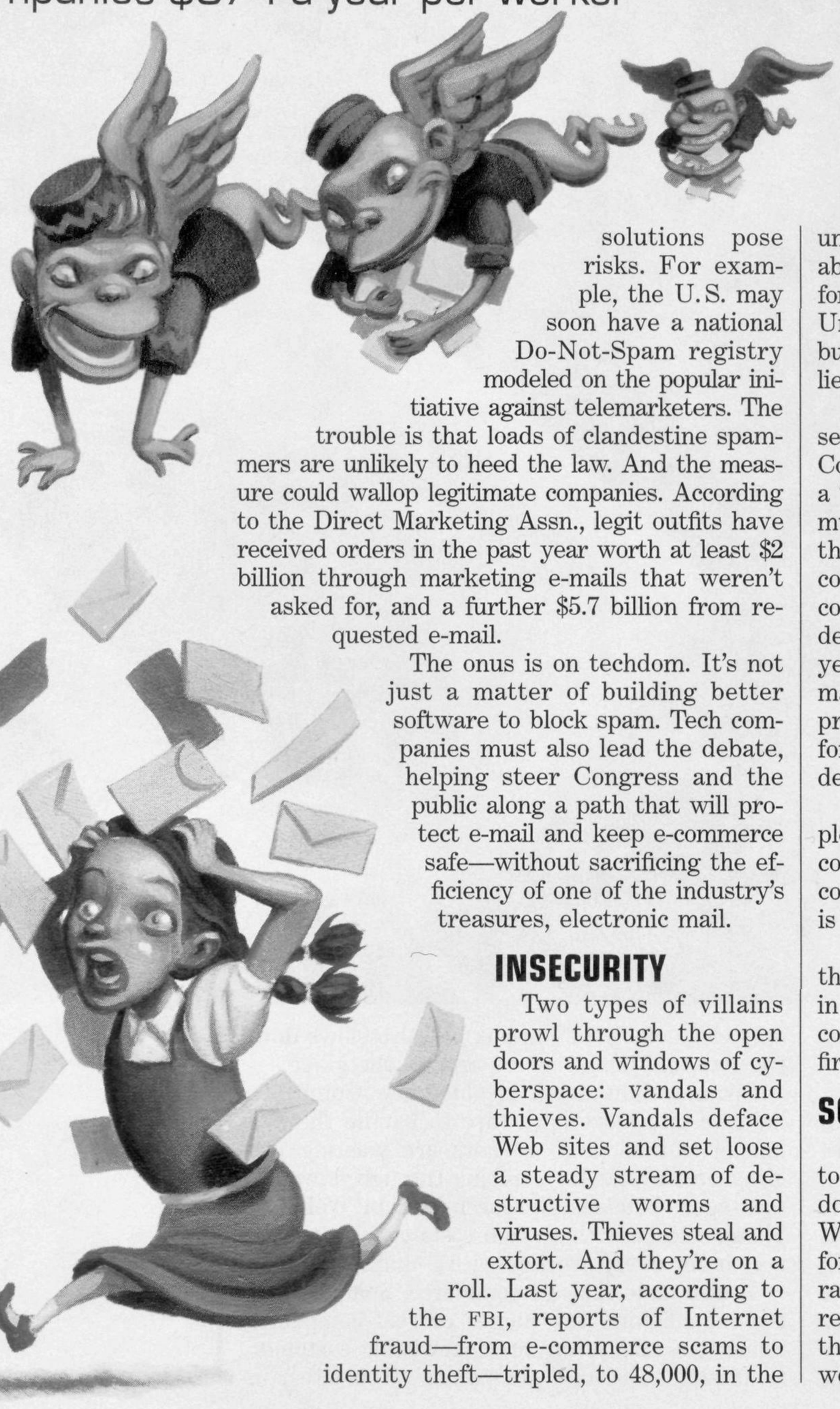
cluding retailer Best Buy, Wells Fargo, and eBay. The goal: to coax credit-card numbers from the victims. Few people report falling for the trick, says the FBI. Yet even those who sidestep danger come away with the message that the Net, teeming with grifters, is a risky place to shop. That message—poisonous for tech—gets reinforced when they purge their spam every day.

Solutions? There are plenty of them, from new legislation to outlaw false headers on e-mail messages to spam-blocking technologies that send junk mail straight into the trash. But even the solutions pose risks. For example, the U.S. may soon have a national Do-Not-Spam registry modeled on the popular initiative against telemarketers. The trouble is that loads of clandestine spammers are unlikely to heed the law. And the measure could wallop legitimate companies. According to the Direct Marketing Assn., legit outfits have received orders in the past year worth at least $2 billion through marketing e-mails that weren't asked for, and a further $5.7 billion from requested e-mail.

The avalanche of spam may be costing companies $874 a year per worker



The onus is on techdom. It's not just a matter of building better software to block spam. Tech companies must also lead the debate, helping steer Congress and the public along a path that will protect e-mail and keep e-commerce safe—without sacrificing the efficiency of one of the industry's treasures, electronic mail.

INSECURITY

Two types of villains prowl through the open doors and windows of cyberspace: vandals and thieves. Vandals deface Web sites and set loose a steady stream of destructive worms and viruses. Thieves steal and extort. And they're on a roll. Last year, according to the FBI, reports of Internet fraud—from e-commerce scams to identity theft—tripled, to 48,000, in the U.S. Reported damages climbed to $54 million, but the real tally is presumed to be far greater. FBI Director Robert S. Mueller III estimates that two of every three fraud cases go unreported. And he has listed cybercrime as the FBI's third-ranking priority, behind only the war against terror and counter-espionage.

Even powerful companies are proving vulnerable. Early this year, a software worm launched by a vandal infected the systems at Bank of America, bringing down 13,000 automated teller machines. Weeks later, a hacker broke through the security system at Data Processors International Inc., an Omaha credit-card processor, and made off with account information on up to 8 million cards. Such thieves, says Bill Murray, a spokesman for the FBI's cyber division, often sell stolen credit-card numbers on black-market Web sites for $1 apiece. "They put up the sites for a day, do their business, and then disappear," says Murray.

Lots of software flaws, or bugs, provide ports of entry for thieves and vandals. Charles C. Palmer, head of IBM's computer-security unit, says that roughly six new software vulnerabilities are reported each day to CERT, a center for Internet security expertise at Carnegie Mellon University that compiles industrywide stats on bugs and hacker attacks. By 2005, Palmer believes, the number could swell to 64 a day.

Technology leaders are starting to grapple seriously with security. A year ago, Microsoft Corp. Chairman William H. Gates III announced a "trustworthy computing" drive. He shut down much of software development for 10 weeks so that employees could take security-training courses. And Microsoft's next operating system, code-named Longhorn, should have far sturdier defenses than Windows when it's released next year. Steven M. Bellovin, top network-security maven at AT&T Labs Research, says he's impressed with some of Microsoft's security efforts, but cautions that they will take years to develop and be deployed.

Even with secure systems, users can create plenty of vulnerability. They routinely log on to corporate networks through undefended home computers. Worse, the most common password is ... PASSWORD.

To create systems safe enough to host much of the world's economy, tech companies must build in bullet-proof security from the get-go—and convince the public to lock their computers as firmly as they bolt their front doors.

SQUEEZED BROADBAND

Who most enjoys a fat broadband connection to the Internet? That's easy. The people who download massive music and film files from the Web, most of it pirated. Sadly, the legal offerings for broadband, from streaming video to Internet radio, are not nearly as compelling. That's one reason the migration to speedy connections in the U.S. has been slow: Dial-up connections work fine for the No. 1 Internet application, e-