

THE HIGH COST OF P2P ON THE ENTERPRISE

In their private lives, prudent people adjust their behaviors based on their perception of risk. Depending on where they live, for example, they lock their doors at night, turn on exterior lights, or maybe even switch on an alarm system. So why, in the face of such obvious risks, would any company unwittingly leave its network wide open and allow the world-at-large to march uninvited and unmonitored through its data pipes? Yet that's exactly what enterprises are doing by not protecting their networks against two of the most popular, fastest growing and potentially menacing applications on the Internet today: peer-to-peer (P2P) and Internet Messaging (IM). Not only is the use of these applications costing enterprises thousands of dollars each year in lost productivity and degraded network performance, but some enterprises have lost millions more in intellectual property theft, steep regulatory fines and liability lawsuits stemming from copyright infringement and sexual harassment activities that went on undetected over corporate networks.

A Growing Problem in Corporate America

A P2P network essentially functions just like an enterprise intranet that enables employees to share corporate information. But where an intranet is private, the P2P network is public, enabling anyone who downloads the network's P2P client software to access files on any other network participant's computer. Similarly, instant messaging networks provide real-time chat functions, along with ancillary functions such as video conferencing and file-sharing. Unfortunately, the real problem with P2P and IM traffic is that they can easily bypass corporate firewalls and other security mechanisms, leaving the network exposed to hackers, viruses, bandwidth waste, legal liabilities and more.

By now it is a well-known fact that P2P file sharing has reached almost epidemic proportions on high school and college campuses. According to a recent survey of 1,000 college students commissioned by the Business Software Alliance, 69 percent have downloaded music, 26 percent downloaded movies, and 23 percent have downloaded software. What may surprise you, however, is the speed at which the problem has proliferated corporate America, as more and more employees count on their employer's high-speed Internet connection to access the large music, video, and software files that are common to P2P networks.

According to a global survey recently released by IDATE (www.idate.fr), close to 60 billion files were downloaded over P2P networks in 2003, 50 to 60 percent of which were downloaded during daytime business hours. In the U.S. alone, according to a survey published by the Pew Internet and American Life Project, an estimated 29 percent of Internet users -- 35 million adults -- use file-sharing software. The growth trends are equally steep for IM, which allows users to communicate in real time with each other and to share files. According to a 2004 Osterman Research survey, up to 70% of enterprises say they have authorized and/or unauthorized public instant messaging applications installed on their network.

Network and Information Security Breaches

P2P and IM clients create major holes in an otherwise sound network security plan. These holes can bring malicious content onto the network and also let sensitive corporate content leak out. Although P2P and IM client software enables users to select which information files they make available for sharing, these controls are easily bypassed or misapplied by users. Meanwhile, their unencrypted communications and use of public/third-party network hubs make them vulnerable to eavesdropping and other forms of electronic theft. Since these programs operate outside normal IT controls, even a single P2P or IM application on a user's computer can leave critical corporate assets exposed to the world, including financial records, customer and patient data, intellectual property and more.

P2P and IM networks also provide an easy point of entry for so-called "Trojan horse" programs,. These programs may be part of the client application (especially true for P2P clients) or masquerade as harmless downloadable content. Once opened, they may silently provide the sender with varying degrees of access and control over the recipient's computer, network and information resources. If one considers the corporate firewall as the wall around the castle blocking unwanted visitors, then the Trojan horse is the ladder invaders use to scale those walls. According to a recent article on eSecurity Planet, recent P2P-based Trojan horse programs such as PWSteal.Reanet have attempted to steal information from online banks and other financial institutions. (eSecurity Planet "P2P Worm Spreads via KaZaA File-Sharing Network", Oct 14, 2003.

Other rogue programs have the ability to record filesharing peers' keystrokes--or those of anyone anywhere on the corporate network--identifying passwords, for example, that could be used for penetration of otherwise secure information resources. The Fizzer worm, for instance, discovered in May 2003, targets users of the KaZaA P2P network who download shared files from an infected machine. The worm contains a denial of service attack tool to freeze target workstations, a data stealing Trojan horse program that can be used to open a path for theft of intellectual property, an HTTP server, auto-updating capabilities, and the ability to disable selected antivirus programs--all of which can severely impact business operations.

Like those in P2P applications, IM packets are able to sneak by firewalls and open the door to corporate network resources, leaving the network, and its contents, entirely unsecured. IM is also equally vulnerable corruption by rogue programs, numerous examples of which have already been identified and documented by the CERT® Coordination Center (www.cert.org) of Carnegie Mellon University's Software Engineering Institute, a major reporting center for Internet security problems that is funded primarily by the U.S. Department of Defense. Although federally funded and private industrial groups work judiciously to document security breaches associated with P2P and public IM, by nature they may be too little too late.

Bandwidth and Productivity Waste

Aside from the potentially high costs of network security breaches, the day-to-day impact of P2P and IM activities can hit a company's bottom-line. With audio and video clips commonly as large as 700 MB, file transfers can take up to two hours to complete, even over high-speed broadband connections. A single P2P network user, for example, can easily consume the full bandwidth of a T1 connection that costs in the range of \$1000 per month. IM users engaging in inappropriate video conferencing can have a similar impact. As a result, corporate networks, -- and employee productivity -- can slow to a crawl. Industry estimates vary widely as to the loss of productivity associated with P2P and IM. While employees surf P2P networks, download files or instant message friends and relatives, work simply does not get done. Some industry pundits have suggested that giving employees uncontrolled access to these communications media is like establishing a business practice that allows for unlimited coffee breaks.

New Liability Risks

Ironically, as the exploding growth in popularity of P2P and IM applications make it increasingly difficult for enterprises to control what happens on their networks, enterprises have become increasingly liable for network activity. In April of 2002, for example, the Recording Industry Association of America (RIAA) reported a \$1 million out-of-court settlement with Integrated Information Systems (IIS), a business and technology consultancy in Tempe, Arizona, because the company allegedly allowed employees to swap copyrighted songs. More recently, in March 2003, the RIAA sent letters to 300 U.S. companies with employees engaged in "illegally distributing copyrighted music on the Internet." These companies are now in direct jeopardy, facing the potential for statutory damages, under Title 17 of the United States Code, ranging from \$750 to \$150,000 for each copyrighted work that has been illegally copied or distributed by their employees.

New legislation will only make copyright violation prosecutions by users of P2P networks and IM easier. Already, for example, a new bill called the Author, Consumer and Computer Owner Protection and Security Act of 2003 has been proposed in Congress that would boost the Justice Department's copyright crime fighting budget 50 percent and institute penalties of up to \$250,000 and up to five years in prison for uploading just one file of copyrighted content. This Act would serve to strengthen the existing Digital Millennium Copyright Act of 1998 which copyright holders can use to identify suspected violators, and thereby place the companies where they work at clear risk.

Of course, enterprise liability for network activity extends beyond copyright infringement. According to the American Management Association, a number of Fortune 1000 companies have recently had to defend themselves against liability claims ranging from sexual harassment, insider trading, and confidentiality breaches stemming from employee misuse of corporate e-mail and Internet systems.

Government Regulations

In addition, several recent regulations have imposed special information controls on healthcare, financial and public companies. These include the Health Insurance Portability and Accountability Act (HIPPA), the Sarbanes-Oxley Act and the recently proposed Government Internet Security Act. Under these regulations, enterprises and state or federally-funded entities must implement and comply with even more stringent Internet Usage Policies or face steep fines and other penalties.

HIPPA, passed in 1996, includes a number of provisions aimed at protecting patient privacy, among them the requirement for administrative procedures that protect data integrity and confidentiality. In providing this protection, HIPPA specifies the need for data integrity and data access controls with full user and message authentication and message encryption capabilities; audit trails and event reporting are also mandated. But neither P2P nor IM communications can meet these standards because users cannot be authenticated, traffic cannot be encrypted, and illicit access cannot be guaranteed. As P2P and IM applications operate outside normal procedures for authentication, security and auditing, their presence on a network can easily compromise an organization's compliance. This means that any healthcare institution or facility allowing employees to access these applications will, quite simply, run the risk of breaking the law and exposing themselves to substantial penalties.

The same holds true for violators of Sarbanes-Oxley. Passed in 2002, this Act requires public companies to implement controls and procedures that ensure accurate reporting of material information affecting the company, and to deploy internal controls to communicate, store and protect that data; companies are also required protect these controls from internal and external threats and unauthorized access. But again, as with HIPPA compliance, if companies allow their employees to engage in unfiltered communication and file sharing activities, they will not be able to meet this mandate since both P2P and IM open communications paths that could compromise corporate standards.

New Attitudes Towards Internet Content Filtering

While more than half of all companies have had to discipline or even terminate employees for inappropriate use of the Internet, many are finding that even the strictest network usage policies are difficult to enforce and can leave them exposed. For many, the only way to effectively minimize the risks and regain control of their networks is to implement an Internet content filter with robust P2P blocking features. While most companies have already implemented some sort of URL filtering, P2P and IM applications have raised new requirements that aren't handles by traditional URL blocking technologies. More and more companies are waking up to the reality that specialized P2P and IM filters are essential to protect and control use of their valuable network resources. A survey published in the July 2003 issue of Inc. Magazine, for example, indicated that 37 percent of companies have already implemented filters to block access to file sharing sites, with many more currently evaluating or considering a P2P blocking solution. In

fact, the Radicati Group estimates the Internet content filtering market will grow from \$653 million in 2003 to \$2.4 billion in 2007, largely because of the recent media attention on the risks associated with P2P, IM and chat applications.

P2P and IM filtering can prevent file sharing activities that can wreak untold havoc on corporate data, significantly slow, or even-stop, corporate networks from operating, expose companies to potentially crippling fines and legal suits, dramatically cut employee productivity, and open a path that facilitates theft of intellectual property. Whether propagated by an outside hacker with a Trojan horse program, by a disgruntled employee seeking revenge, or by someone seeking payment for trade secrets, IM or P2P is a virtual free pass: no file sharing filter, no way to track or stop the loss of information and network corruption.

Companies invest billions of dollars each year in network security. Yet the presence of uncontrolled P2P and IM applications may render much of that investment worthless. A flexible Internet filter that can monitor, report on, and control all file sharing activities may be the only way for an enterprise to dramatically minimize, if not eliminate, these new and dangerous risks. With most Internet filters priced between \$10 and \$30 per workstation, the cost of an Internet filter is a truly insignificant price to pay for the protection it brings.