

FEATURE

Supermarket chain FREEZES Internet access

Audit of network usage at Balls Food Stores confirms that tight policies are working to limit unauthorized Web surfing.

BY JOEL SHORE

Emloyees of the Balls Food Stores chain don't download music or video files. No one listens to Internet radio or accepts e-mails with large attachments. And, to an amazing degree, employees only visit Web sites directly related to corporate business.

Call it Midwest sensibility, outright paranoia or the direct result of extraordinarily tight-fisted control, the Kansas City, Kan., operator of 28 Hen House and Price Chopper supermarkets and pharmacies is the very model of how a network — and its users — should behave. Not that the users really ever had a choice.

Balls Food's remarkable network usage, documented in an audit performed recently by Networks Unlimited of Hudson, Mass., is the

product of restrictive policies that grant Internet access to employees on a case-by-case and site-by-site basis and by aggressive filtering of inbound and outbound e-mail.

How aggressive? Send out an e-mail with an inappropriate attachment and your e-mail privileges might be suspended for a week.

"I'm relieved at the [audit] results," says CFO Mike Beal, who stands firmly behind the policy.

Harry Segal, president of Networks

Unlimited and a veteran of dozens of usage audits was equally surprised. "These results are unusually good."

Usage audits look for exposure in four areas: productivity loss, legal liability, bandwidth consumption and data security.

Balls Food did well in all four. Most users can't get to shopping, auction or sports Web sites, so there's little lost productivity. Likewise, the inability to access objectionable content minimizes legal exposure. Unable to con-

nect to Internet radio streams or download multimedia files, bandwidth is preserved. Finally, spyware, Trojans, viruses and keystroke loggers are kept out through aggressive e-mail filtering and Web download prohibitions, assuring the security of sensitive data.

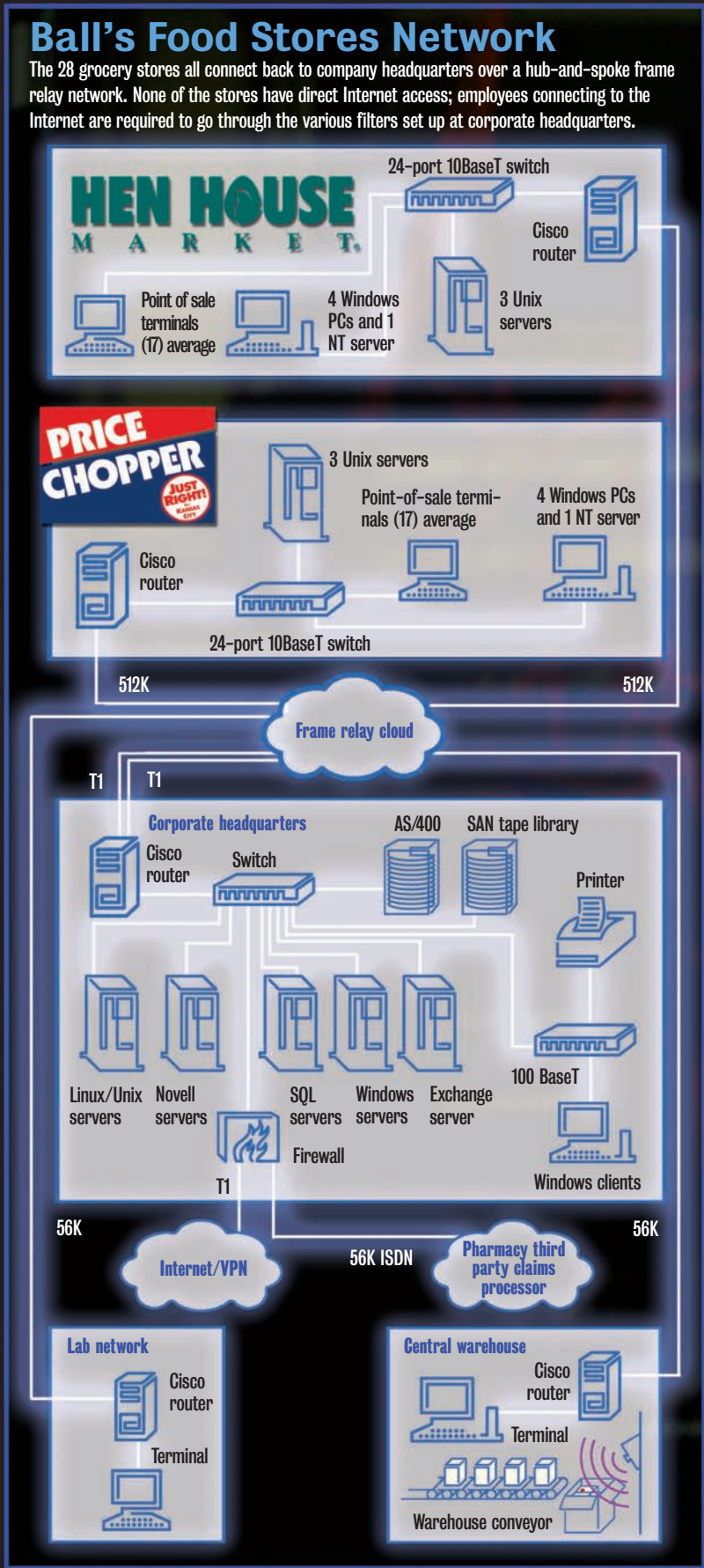
"If we had an open Internet policy, our problems would be much worse," says Lance Fischer, Balls Food's network systems manager. "Our policies and practices are well-established, known by every employee with a computer and strictly enforced." To Fischer, it's mostly about enforcement.

The policy is hammered home every time a user logs on to the network. As part of the login process, users are presented with a dialog box summarizing the policy and reminding them that "the use of this system may be monitored and recorded for administrative and security reasons." To proceed, a user must agree by clicking the OK button.

To assure that it has complete control, Balls Food's network has a "wagon wheel" configuration, with the central office as the hub and the stores as spokes. All traffic moves through the hub and all data is stored at the hub. The point-of-sale system, owned by a different corporate department, runs separately.

With nearly 3,000 employees and a PC population of about 350, roughly 15 people in each of its 28 store locations and 100 at its headquarters have Internet access. To maintain the tightest control possible, access is available only by using the corporate intranet as a gateway. The scheme allows Fischer's team to specify the IP addresses of permitted Web destinations to the firewall.

News, sports, entertainment and shopping sites are banned outright. Specific sites that are allowed include those furnishing local weather forecasts, highway traffic reports, the employee assistance program, 401 (k) account-status information, drug-screening and background check sites for employee candidates, and direct line-of-business sites such as grocery suppliers and wholesalers.



“Other companies give their employees full Internet access and take it away when there is a problem,” Fischer says. “Our attitude is, ‘Don’t give them anything that’s not required to do their job.’”

The one exception is that the pharmacies have unlimited access, because pharmacists need to research potential interactions between prescription drugs and over-the-counter or mail-order remedies.

And it’s precisely because of that exception that the audit results weren’t perfect.

“Right away, I could see those machines were being used to log into Hotmail and other Web sites,” Fischer says. Web-based personal e-mail sites are Fischer’s favorite target. “With Hotmail or Yahoo there’s no control over what comes in. We try to block multimedia files.”

And with good reason. “In December, people would receive an e-mail with a Christmas tree that you could click on to decorate. It looked innocent enough, but it wound up installing a keystroke logger on people’s computers.”

That’s bad enough, but when the keystroke logger is on a PC in a pharmacy that is already struggling to keep up with Health Insurance Portability and Accountability Act (HIPAA) privacy mandates, the potential for legal exposure skyrockets. “A keystroke logger is a clear HIPAA violation,” Fischer says.

Tools of the trade

Balls Food uses the Perimeter Manager preemptive e-mail filtering service from Postini for its corporate system. Incidents of spam quickly dropped to nearly zero, but Fischer especially likes the ability to keep viruses and SMTP attacks from ever reaching the enterprise gateway.

Postini’s presence also led to the suspension of one employee’s e-mail privileges. As he scanned outgoing e-mail, Fischer noticed unapproved attachments being sent — attachments that could not have entered through the Postini-protected corporate e-mail system. The source turned

out to be a personal Hotmail account, accessed by an employee who then relayed the content through the company’s Microsoft Exchange Server.

“We shut down someone’s e-mail for five days,” Fischer says. “Losing the ability to send legitimate mail caused a lot of grief.” Draconian perhaps, but the measure did not need to be repeated.

Inside the audit

To measure user activity, Networks Unlimited employed a server on which it installed Websense, configured as a passive logging tool that performed no filtering action of its own. Segal shipped the server and an engineer to Kansas City to install it.

Network activity for a representative group of pharmacies and headquarters PCs was logged for 11 consecutive days. The server was then shipped back to Networks Unlimited for analysis. Data was extracted and annualized totals were extrapolated; each hour of logged activity over the audit period scaled to 33 hours over the course of a full year. Following compilation of the results, Segal flew to Balls’ headquarters to present his findings.

On an annualized basis, Balls employees behaved far better than counterparts at other similarly sized companies audited by Networks Unlimited.

Where Balls staffers spent just 686 hours accessing Web-based e-mail, workers at a midsize medical center wasted 1,477 hours, while employees at a similarly sized law firm squandered 6,525 hours.

The law firm logged visits to dozens of gambling sites, with activity dipping during lunch and plummeting after 6 p.m. There’s only one interpretation, according to Segal: “They’re visiting these sites during working hours.” At the law firm, the top source of downloaded streaming media was espn.com. At another law firm, identical time-of-day usage patterns were noted for sites featuring adult content. The conclusion was that employees are surfing when they should be working, and they rarely skip lunch.

Where Balls reported no Internet radio streaming downloads, the law firm, dur-

ing its one-week audit period, logged more than 3G bytes of streaming content. That one non-business-related activity works out to more than 156G bytes over the course of a year.

At Balls Food, employees spent 429 hours at personal shopping sites, compared with a slightly more than average 2,073 hours by staffers at the medical center.

“There can be no doubt that because Balls started with a closed policy, it has maintained control and protected its network, data and the company itself,” Segal says.

With dozens of audits performed over the last two years, Networks Unlimited is seeing personal usage patterns change significantly. Peer-to-peer activity, once typified by download services such as Napster, has dropped steadily, while instant messaging use has risen dramatically. Visits to sites featuring adult content have remained largely constant.

More to do

Despite the restrictive policies that prohibit access to all but a handful of carefully chosen Web destinations, Balls Food is about to embark on a corporate-wide deployment of the Websense security and filtering platform. Its policies already running contrary to conventional thinking, Fischer, perhaps not surprisingly, takes a contrarian view of Websense, too.

“Most companies use Websense to clamp down on employee Internet activity. We’ll do the exact opposite; I see it as a way to gradually widen Internet access,” he says.

Fischer is realistic enough to know that Balls’ policy of granting access on an employee-by-employee and site-by-site basis simply doesn’t scale up for corporations with thousands of employees.

“What these companies must do is actually enforce their electronic use policies and prohibit access to anything that wastes company resources or endangers the network,” Fischer says.

Shore is a technology journalist in Southborough, Mass., who provides product-strategy consultation and editorial-development services to technology companies. He can be reached at www.joelshore.com.