

SECURE ENTERPRISE

BUILDING TRUSTED BUSINESS

June 2004

[SPECIAL REPORT]

OUTSOURCING GOES MAINSTREAM

For security, the risks in not outsourcing may be worse than the alternative

By Anne Zieger



Outsourcing your network defenses may seem like an odd idea. After all, doing so means handing over the keys to your enterprise to some stranger. Yet security outsourcing is becoming popular to the point of becoming a fad. As the pace of network attacks accelerates and as Internet applications and services extend cyber risk across a web of partners, enterprises are turning to outsiders with expertise in key areas of security.

In fact, enterprises will spend \$5.9 billion on managed security services in 2007, up from \$1.6 billion in 2002, according to research firm In-Stat/MDR. And it's no wonder. The General Accounting Office, the audit and investigative arm of Congress, estimates that companies will lose as much as \$50 billion this year as a result of cyber attacks.

For PMI Mortgage Insurance Co., bringing in an outsourcer was regarded as the best way to supercharge the effectiveness of its IDS (intrusion-detection system), according to officials at the Walnut Creek, Calif., company. As PMI's business grew more dependent on the Internet, executives felt increasingly exposed. Managers knew that industry best practices called for a robust IDS, but the company's IT leaders realized they didn't have in-house intrusion-detection experts, and they didn't want to commit to hiring the six to eight staffers they would need for round-the-clock monitoring.

"An IDS without 24/7 coverage is an inadequate solution," says Todd Berman, team lead for information security. "We felt that hiring an outsourcer for that would be more effective from a cost perspective and also would get us high-quality individuals." Now the company's IDS is managed by Counterpane Internet Security. As Berman sees it, Counterpane is in a much better position than he is to spot threats before they can do damage. That's because Counterpane is monitoring traffic on as many as 400 user networks all the time. "If they see exploits traveling across the Web, they can update signatures long before we can," Berman says.

PHOTOGRAPH BY (PETER HOLST)/GETTY IMAGES



A SECOND SET OF EYES

Security outsourcing takes many forms, from quarterly vulnerability assessments at the low end to round-the-clock monitoring and management of security applications at the high end. Many security providers offer 24/7/365 monitoring of key defensive systems, security-breach tracking and responses to Internet virus events or attacks. The prices for this type of service vary widely but typically fall in the range of \$25,000 to \$50,000 per year, industry researchers say. Periodic vulnerability assessments run around \$100 per server.

Providers also have emerged to address e-mailed threats. They monitor e-mail continuously for spam and inappropriate content. These services, an alternative to spam filtering appliances that can cost up to \$7,000, may run as little as a dollar or two per employee or as much as \$10 per employee per month.

Small and midsize companies (fewer than 5,000 employees) seem especially interested in hiring outside defenders. Even those companies that can afford dedicated security staffs find value in having outside specialists check their work. "Companies are budgeting for things that need a second set of eyes ... things that they might be able to do internally but are better to have someone outside do," says Michelle Drolet, CEO of Holliston, Mass., IT security consulting firm Conqwest, which

provides vulnerability scanning, security-policy development, education and technology assessment for small enterprises.

Salaries for security professionals have skyrocketed because of a shortage of skilled workers. Only a few thousand people have Ph.Ds and some 15,000 have master's degrees in information security, says Burton Group analyst Fred Cohen. "In some cases, no matter what you do you can't get one," he says, so sharing security talent with other IT shops seems sensible. "There aren't even enough CISSPs to cover the *Fortune* 500."

Beyond the labor shortage, some companies simply can't stomach having to retrain staff every time a new threat emerges. Such was the case when law firm Harness, Dickey & Pierce decided to hire an outsourcer firm to battle spam on its behalf. The firm, whose 274 lawyers and staffers specialize in intellectual property, hired Postini, an application service provider that monitors and filters the firm's incoming e-mail day and night. The firm pays \$545 per month for Postini's service, which covers 302 e-mail boxes. For that fee, Postini intercepts all of the firm's e-mail and filters out spam before routing the mail to Harness Dickey's e-mail server.

For the firm's IT leadership, the decision to outsource was more instinctive than anything else. "We didn't do a thorough quantitative cost analysis," says Hector Cruz, Harness Dickey's director of information services. "We weighed the difficulty of performing these services ourselves versus outsourcing, and we determined that a third-party e-mail filtering service would be cheaper than the professional time wasted dealing with unwanted spam."

The Burton Group's Cohen says the downside to hiring outsiders to battle spam is that they have access to all your precious e-mail. "So much for confidentiality," he says.

NOT JUST FOR LITTLE GUYS

Even some large companies with sophisticated IT organizations are opting for outside security experts. They include Steelcase, a *Fortune* 500 office products company with 16,000 employees and

an IT staff of more than 300. A few years ago, IT managers decided they'd have a more bulletproof firewall if an outside expert would look over their shoulders as they updated and changed configurations.

Steelcase has worked with several security consultancies over the years. Today the company works with Belgium-based managed services firm Ubizen, whose OnlineGuardian service monitors network- and application-level security components 24/7. Ubizen operates a U.S. headquarters in Reston, Va.

Now, when Steelcase's IT staff seeks to make firewall configuration changes or implement patches, they must contact Ubizen, which reviews and double-checks each change before approving it. Mostly that means making sure that requested changes don't conflict with existing configurations. "We wanted tight control for changes in the configuration, and we didn't think we could do it as well internally," says Paul Prentice, manager of security and directory services for the Grand Rapids, Mich., manufacturer. "You can make a strict policy, and at first, people will be good about it, but they get lax about changes eventually."

Of course, each company must make its own outsourcing decision, and like all things security, it's a question of your risk tolerance. Outsourcing means entrusting your valuable intellectual assets to an outsider. But the alternative might be to trust an underqualified employee with the task.

WRITER: ANNE ZIEGER

ANNE ZIEGER IS A FREELANCE BUSINESS AND TECHNOLOGY EDITOR BASED IN ALEXANDRIA, VA.



CAN OUTSOURCING REALLY SAVE YOU MONEY?

Ask any security consultant, and he or she will tell you that outsourcing will save you money. And it seems to make sense: By sharing the cost of security experts with other clients, you pay only fractions of their salaries rather than full ones.

In fact, it would take as many as six full-time security staffers, at an annual cost of about \$200,000, to duplicate the services a managed service provider like Counterpane Internet Security can deliver at \$25,000 to \$50,000 per year, according to Bruce Schneier, CTO of Counterpane.

But Bill Johnston, president of ROI consultancy Alinean, throws a grain of salt into this recipe. He says it's just not realistic that an IT shop would hire six security experts to provide round-the-clock coverage for network monitoring. In his experience, consultants usually can deliver the same monitoring services at roughly 80 per-

cent of the cost of hiring in-house staff. Often, the remaining 20 percent is eaten up by profit margin, he says, making the costs roughly equal.

"If you're already running an operation with 24/7 coverage, you can usually do it internally because you have the people," Johnston says. If you don't, ramping up to full-time coverage can be costly, and the true costs may come closer to Schneier's claim, he says.

Even so, Schneier's business case doesn't take into account that full-time workers, particularly highly trained ones, often will innovate during their downtime, adding unanticipated value to their jobs. It's the difference between an expert working with you versus an expert working for you.

Another way to calculate the payback of security outsourcing is to weigh the risks of not farming it out. For example, if your company typi-

cally suffers two virus incidents per year, at roughly \$25,000 per incident, that's about \$50,000 in exposure per year. Looked at that way, Johnston notes, you can spend up to that amount per year and still save money.

Outsourcing also may be the only way for financial services and health-care companies to comply with Sarbanes-Oxley and the Health Information Portability and Accountability Act, respectively, says Burton Group analyst Fred Cohen. Both laws impose heavy fines for not adequately protecting customer records.

"If you think people with a couple of years' experience can do as good a job as information security professionals, you're making a big mistake," Cohen says. "A lot of people find out how big a mistake they've made when there's an information leak—and face going to jail."