



Counterpane™
Internet Security

Why Outsource?

Bruce Schneier, Founder & CTO



Introduction

More and more companies are outsourcing their network security. This trend is driven by one truism: there is no other way to deal with the shortage of skilled computer security experts, the increasing requirements for businesses to open their networks, and the ever-more-dangerous threat environment. For the Internet to succeed as a business tool, security has to scale. Outsourcing is how it will do that. This has always been Counterpane's fundamental business model.

But if the decision to outsource network security is a difficult one, the decision of precisely what to outsource seems impossible. Managed security service companies can monitor your networks, manage your security devices, scan your networks, implement your security policies, install your security devices, and more. Other companies offer similar services, often tied to particular products or suites of products. And sometimes outsourced network security comes in a package with other outsourced network services.

On one hand, the promises of outsourced security are very attractive: the potential to significantly increase your network's security without hiring half a dozen people or spending a fortune is impossible to ignore. On the other hand, giving over your network security to another company feels like it should be inherently risky.

In reality, there's no dichotomy. Hiring Counterpane to handle your network security can be less risky than building your own expertise inside your company. And it most definitely can be both cheaper and more effective. You already understand why; you just might not have thought of it in terms of network security.

Arguments for Outsourcing

The primary argument for outsourcing is financial: a company can get the security expertise it needs much more cheaply by hiring someone else to provide it. Take monitoring, for example. The key to successful security monitoring is vigilance: attacks can happen at any time of the day and any day of the year. While it is possible for companies to build detection and response services for their own networks, it's rarely cost-effective. But Counterpane already has that expertise.

Staffing for security expertise 24 hours a day and 365 days a year requires five full-time employees—more, if you include supervisors and escalation personnel with specialized skills. Even if an organization could find the budget for all of these people, it would be very difficult to hire them in today's job market. But if you think hiring them is difficult, retaining them would be an even harder challenge. Security monitoring is inherently erratic: six weeks of boredom followed by eight hours of panic, then seven weeks of boredom followed by six hours of panic. Attacks against a single organization don't happen often enough to keep a team of the caliber needed engaged and interested. This is why outsourcing is the only cost-effective way to satisfy the requirements.

Medical care is a prime example of outsourcing that we can use for comparison. Everyone outsources healthcare, in the sense that we don't act as our own doctor, nor does anyone hire a private personal doctor. Certainly cost is a factor in our decision to outsource, but there's more to it than that. I may only need a doctor twice in the coming year, but when I need one I may need him immediately, and I may need specialists. Out of a hundred possible specialties, I may need two of them—and I have no idea beforehand which ones. I would never consider hiring a team of doctors to wait around until I happen to get sick, so I outsource my medical needs to my clinic, my

emergency room, my hospital. Similarly, it makes sense for a company to outsource its network security needs to a variety of experts.

The benefits of security outsourcing are enormous. Aside from the aggregation of expertise, an outsourced monitoring service like Counterpane's has other beneficial economies of scale. We can more easily hire and train its personnel, simply because we need more employees and it can build an infrastructure to support them. We also have a much broader view of the Internet. We can learn from attacks against one customer, and use that knowledge to protect all of our customers. And from our point of view, attacks are frequent. Vigilant monitoring means keeping up to date on new vulnerabilities, new hacker tools, new security products, and new software releases. We can spread these costs among all of their customers.

To return to our medical care analogy, you get better medical care from a doctor that sees patient after patient, learning from each one. To an outsourced security company, network attacks are everyday occurrences and its experts know exactly how to respond to any given attack, because in all likelihood they have seen it many times before.

What to Outsource

There are, however, limits on what you should outsource. The bottom line is that you won't outsource everything, because some things just don't outsource well. Things that don't outsource well are often too close to your business, or they're too expensive for an outsourcing company to deliver efficiently, or they simply don't scale well. Knowing the difference is important.

Think about healthcare again. We all know what aspects of medical care we like: the ambulance picks us up in seconds and rushes us to the hospital, a team of medical experts spares no expense in running tests to figure out what's wrong and in doing whatever it takes to cure us. And we all know what aspects we don't like: ill-equipped and ill-staffed hospitals, HMOs telling us that we can't have that particular test or that a specialist isn't warranted in this case. The aspects of outsourced healthcare we like involve immediate access to experts. Any medical emergency requires experts, and the faster they can pay attention to us, the better off we'll be. The aspects of outsourced healthcare we don't like involve control of the process. Our healthcare is our responsibility, and we don't want someone else making life and death decisions about us. Network security is no different. Outsource expert assistance: vulnerability scanning, monitoring, consulting, forensics. Don't outsource control of the process.

At Counterpane, we monitor networks. We manage firewalls, IDSs, and IPSs. We provide vulnerability scanning, e-mail and web scanning, and "clean-pipe" Internet connections. We have the expertise to deal with compliance issues. We can build a whole new security infrastructure for you from the ground up. In short, we can take the problems of network security off the backs of a corporate IT department and let them focus on their strategic decisions.

What we cannot do is determine how their IT security interacts with their business. For example, we can detect when a hacker is inside a corporate network and what he's doing, but we won't know the business ramifications of different responses. We can detect an insider attacking your network, but we don't know whether he's malicious or performing authorized testing. We have customers who run highly secure networks, and would rather disconnect from the Internet than have a hacker wandering around. We have other customers who generate far too much revenue from their Internet connection to disconnect for even a minute, and require responses that keep them operational. We

work best when we can work with our customers, combining our expertise with their knowledge of the business processes.

How to Choose an Outsourcer

Choosing an outsourcing partner is difficult, because it's hard to tell the difference between good computer security and bad computer security. But by the same token, it's hard to tell the difference between good medical care and bad medical care. If we're not health experts ourselves, we can sometimes be led astray by bad doctors that appear to be good. So how do you choose a doctor? Or a hospital? I choose one by asking around, getting recommendations, and going with the best I can find. Medical care involves trust; I need to be able to trust my doctor.

Security outsourcing is no different; you should choose a company you trust. To determine which one, talk with others in your industry or ask analysts. Go with the industry leader. In both security and medical care, you don't use a little-known maverick unless you're desperate. Watch companies that have conflicts of interest. Some outsourcers both sell products and offer managed security services. This worries me. If the service arm finds a problem with one of its products on my network, will the company tell me, or try to fix it quietly? If they discount their services in an attempt to sell products, who does their services division really work for?

In any outsourcing decision that involves an ongoing relationship, the financial health of the outsourcer is critical. Look for companies that are leaders in their field, have a strong history of security services, and don't try to do everything.

The Future of Outsourcing

Modern society is built around specialization; more tasks are outsourced today than ever before. We outsource fire and police services, government (that's what a representative democracy is), and food preparation (restaurants). In general, we outsource things that have one or more of three characteristics: they are complex, important, or distasteful. In business, we outsource tax preparation, payroll, and cleaning services. Outsourcing security is nothing new: all buildings hire another company to put guards in their lobbies, and every bank hires another company to drive its money around town.

Computer security is all three: complex, important, and distasteful. Its distastefulness comes from the difficulty, the drudgery, and the 3:00 a.m. alarms. Its complexity comes out of the intricacies of modern networks, the rate at which threats change and attacks improve, and the ever-evolving network services. Its importance comes from this fact of business today: companies have no choice but to open up their networks to the Internet.

Doctors and hospitals are the only way to get adequate medical care. Similarly, outsourcing is the only way to get adequate security on today's networks. Counterpane monitors more networks, world-wide, than anyone else, and that number grows constantly. And we can do it better, and cheaper, than our customers can do it for themselves.

For more information, please contact Counterpane's Managed Security Specialists.

Call Us: 888-710-8175

Email Us: info@counterpane.com

Visit Our Website: www.counterpane.com

