Outsourcing security has a lot in common with another vital service—medical care—that we regularly outsource and literally trust with our lives.

The Case for Outsourcing Security

Bruce Schneier, Counterpane Internet Security, Inc.

Deciding to outsource network security is difficult. The stakes are high, so it's no wonder that paralysis is a common reaction when contemplating whether to outsource or not:

- *The promised benefits of outsourced security are so attractive.* The potential to significantly increase network security without hiring half a dozen people or spending a fortune is impossible to ignore.
- *The potential risks of outsourcing are considerable.* Stories of managed security companies going out of business, and bad experiences with outsourcing other areas of IT, show that selecting the wrong outsourcer can be a costly mistake.

If deciding whether to outsource security is difficult, deciding what to outsource and to whom seems impossible. Over the past few years, we've seen many different companies offering different capabilities under the general category of "managed security services." The field is so confusing that even the industry analysts can't agree on how to categorize the services offered. This company manages firewalls. That company offers periodic vulnerability scans. Another offers to manage security policies, or monitor the network, or install the IDS, or host the computers. Some of these businesses make sense, and some of them don't. Some will survive; some won't.

What to outsource

Companies won't outsource everything, because some things just don't outsource well. Either they're too close to the business, or they're too expensive for an outsourcing company to deliver efficiently, or they simply don't scale well. Knowing what to outsource is key.

Medical care is a prime example of outsourcing that works well. Everyone outsources healthcare; we don't act as our own doctor. More to the point, no one hires a private personal doctor. And we all know what aspects of medical care we like: the ambulance arrives 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 (for many people) the insurance company pays (all or most of) the bill. We all also 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, and getting stuck with an outrageous bill.

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 management. Our healthcare is our responsibility, and we don't want someone else making life and death decisions about us.

Network security is no different. Companies should outsource expert assistance: vulnerability scanning, monitoring, consulting, and forensics, for example. But they should not outsource management.

The industry has already proven this point. Salinas Network Services was the largest firewall management company. Earlier this year, it disappeared. There just wasn't a profitable business in managing firewalls for other companies. Firewall management is simply too central—companies outsourcing to Salinas had no choice but to treat their Salinas contractors as employees. And, for the money they were willing to pay, the companies demanded too much individual attention. Another example: Pilot Network Services offered secure network management. Its business was to host computers securely, manage all security devices, and test applications before putting them up on the network, effectively becoming the security management group. They're gone now too—same problem.

Some consulting companies are doing well and some are not. This is primarily a function of the quality of the service they offer. Consulting is, and always will be, a profitable business. Outsourcing occasional requirements for expertise transcends any single area. The outsourced security companies that are doing well offer clearly defined services organizations need. For example:

Managed Security

Giga Information Group is a respected industry analyst; for their report on managed security services, go to www.gigaweb.com/mktg/man_sec_mon/cpane2.asp.

- Consulting companies (such as VeriSign, @Stake, Foundstone) provide expert advice and assistance: strategic security consulting, penetration testing, forensics, and so forth.
- Security Value-Added Resellers (VARs) provide product installation and configuration.
- TruSecure provides certification and expert assistance.
- Qualsys has an automatic vulnerability scanning service.
- Counterpane provides network security monitoring.

In all of these cases, the company buying the security services retains management and ultimate control. Conversely, by not demanding a management role, the security providers offer useful, effective, and scalable services. Both win.

Why outsource security

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, 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.

Staffing for security expertise 24 hours a day, 365 days a year, requires five full-time employees—more when you include supervisors and backup 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.

Retaining them would be even harder. 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 this caliber engaged and interested.

This is why outsourcing is the only cost-effective way to satisfy the requirements. Think about healthcare again. I might only need a doctor twice in the coming year, but when I need one I might need him immediately, and I might need specialists. Out of a hundred possible specialties, I might 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. I outsource my medical needs to my clinic, my emergency room, my hospital. Similarly, companies will outsource network security monitoring.

Aside from the aggregation of expertise, an outsourced monitoring service has other economies of scale. It can more easily hire and train personnel, simply because it needs more employees. And it can build an infrastructure to support them. Vigilant monitoring means keeping up to date on new vulnerabilities, new hacker tools, new security products, and new software releases. Outsourced security companies can spread these costs across all customers.

An outsource company also has a much broader view of the Internet. It can learn from attacks against one customer, and use that knowledge to protect all its customers. It also faces attacks much more frequently. No matter how wealthy we are, we don't hire a doctor to sit in our living room, waiting for us to get sick. We get better medical care from a doctor who sees patient after patient, learning from each one. To an outsource security company, network attacks are everyday occurrences; its experts know exactly how to respond to any given attack, because in all likelihood they have already seen it many times before.

How to choose an outsourcer

It is difficult to choose an outsourcer because it's hard to tell the difference between good and bad computer security. By the same token, it's hard to tell the difference between good and bad medical care. Because most of us aren't healthcare experts, we can sometimes be led astray by bad doctors who appear to be good. So how do we 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; companies should choose an outsourcer they trust. Talking with others and asking industry analysts will reveal the best security service providers. Go with the industry leader. In both security and medical care, you don't want a little-known maverick.

Companies buying security services should also avoid outsourcers that have conflicts of interest. Some outsourcers offer security management and monitoring. This worries me. If the outsourcer finds a security problem with my network, will the company tell me or try to fix it quietly? Companies that both sell and manage security products have the same conflict of interest. Consulting companies that offer periodic vulnerability scans, or network monitoring, have a different conflict of interest: they see the managed services as a way to sell consulting services. (There's a reason companies hire outside auditors: it keeps everyone honest.) Outsourcers offering combined management and monitoring services will be among the next to disappear, I believe. If a company outsources security device management, it is essential that it outsource its monitoring to a different company.

In any outsourcing decision requiring an ongoing relationship, the financial health of the outsourcer is critical. The last thing anyone wants is to embark on a long-term medical treatment plan only to have the hospital go out of business midstream. Similarly, organizations that entrusted their security management to Salinas and Pilot were left stranded when those companies went out of business.

Modern society is built around specialization; more tasks are outsourced today then ever before. We outsource fire and police services, government (that's what a representative democracy is), and food preparation. Businesses commonly outsource tax preparation, payroll, and cleaning services. Companies also outsource security: all buildings hire another company to put guards in their lobbies, and every bank hires another company to drive its money around town.

Continued on pg. 26 ➢

10. D. Davis, "Compliance Defects in Public-Key Cryptography," *Proc. Sixth Usenix Security Symp.,* Usenix Assn., Berkeley, Calif., 1996, pp. 171–178.

11. D.A. Norman, *The Invisible Computer,* MIT Press, Cambridge, Mass., 1998.

12. A. Odlyzko, "The Visible Problems of the Invisible Computer: A Skeptical Look at Information Appliances," *First Monday,* vol. 4, no. 9, Sept. 1999; www.firstmonday.dk/issues/issue4_9/odlyzko/index.html.

Frank Stajano is a faculty member at the Laboratory for Communications Engineering of the University of Cambridge, where he holds the ARM Lectureship in Ubiquitous Computing. His book, *Security for Ubiquitous Computing* (John Wiley & Sons, Chichester), develops in detail the topics touched upon in this article. Contact him at http://www-lce.eng.cam.ac.uk/~fms27/.

Ross Anderson leads the security group at the Computer Laboratory of the University of Cambridge, where he is Reader in Security Engineering. He is the author of *Security Engineering—A Guide to Building Dependable Distributed Systems* (John Wiley & Sons, New York). Contact him at www.cl.cam.ac.uk/~rja14/.

The Case for Outsourcing Security, *continued from p. 21*

In general, we outsource things that have one of three characteristics: they're complex, important, or distasteful. Computer security is all three. Its distastefulness comes from the difficulty, the drudgery, and the 3 a.m. alarms. Its complexity comes out of the intricacies of modern networks, the rate at which threats change and attacks improve, and ever-evolving network services. Its importance comes from this fact of today's business world: companies have no choice but to open 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 for today's networks.

Bruce Schneier, CTO and founder of Counterpane Internet Security, Inc. (www.counterpane.com), has authored six books, including *Secrets & Lies* and *Applied Cryptography* (John Wiley & Sons, New York). He has presented papers at numerous international conferences and is a frequent writer, contributing editor, and lecturer on information security, risk management, and privacy. Contact him at schneier@counterpane.com.