non high-tech areas such people are not available and employers are forced to do with out.

A majority of companies will train employees just to satisfy hiring needs. This often results in a high turn-over rate due to trained individuals leaving to seek greater challenges and better pay. Thus adding value to employees simply raises the cost of keeping a position filled.

A recent trend that addresses these needs while controlling costs are managed firewall and monitoring services.

Like bandwidth service, server management, and web content and design, managed security services are a popular method of reducing the cost of ownership.

There are currently four generations of managed firewall security services.
The first generation is the simple out-sourcing of configuration to an external temporary consultant with the necessary skill set to perform the setup and installation of the required hardware and services.
Second generation managed firewall services are general monitoring and audit/scan services, providing twenty-four hour monitoring and reporting of a site's firewall and connectivity. Configuration and maintenance is done by first generation-style third party consulting services on an as-needed basis.
Third generation managed services consist of one hundred percent outsourcing of firewall management monitoring and maintenance. The customer has little or no access to the day-to-day configuration and maintenance and any changes to the firewall must to be done via customer support services, typically completed within twenty-four hours.
Forth generation services are those that provide total management of the firewall but with a co-management option, thus allowing the customer to maintain both full access and control of their site and the assurance of full monitoring and updating. Based on the policies in place, a customer may have full access

A fourth generation managed security service addresses these problems by providing round the clock monitoring and policy enforcement while presenting a significant savings. This option costs an average of thirty thousand dollars ($30,000) or less per year and includes 24 hour active monitoring, a savings of nearly ninety-five percent (95%).

Another common risk is employee sabotage. A disgruntled employee can sabotage the network parameter or an ex-employee can return via backdoors installed in the network security parameter . These cases are more common then generally perceived since a majority of them are not prosecuted or reported to authorities.

These particular risks can also be avoided with fourth generation managed security services since all changes are reviewed to conform to a set security policy and thus cannot be installed in secret. A managed security service is also bonded and accountable, whereas with individual employee there are often few options short of pressing criminal charges.

Another scenario involves the release of a risky employee, which can be

©Copyright Peter shipley

Why Managed Services?

By: Peter shipley
< Shipley@dis.org >
Draft July 13th 2001[1]

As the costs of in house service rises, the costs of outsourcing drops. As network connectivity, host management and web page content generation, firewall & IDS, managed services are becoming economical and more secure solutions.

When a web page or an Internet site is compromised, the financial loss is not a result of lost revenue or immediate down time but from the follow-up: cleanup, forensics, system reinstallation, site audits and loss of credibility. This can add up to a significant sum of money.

Considering that only six per cent of companies recover from catastrophic data loss, a firewall and network security administrator is a must for any network-connected business. The cost of doing this can be shockingly high since controlling and monitoring access to the Internet site is a 24/7 job requiring trained personal. Running an Internet site without a firewall and network administrator is as risky as giving a teenager a hot-rod for his sixteenth birthday without seatbelts or autoinsurance.

Twenty-four hour monitoring helps to prevent probes from becoming attacks and full site compromises. Plus, it is depressing and a PR disaster to learn about your site's compromise via the media or a call from a customer.

The cost of establishing a secure Internet firewall can easily exceed two hundred and twenty thousand dollars ($220,000) in the first year alone and over one hundred thousand ($100,000) for following years (based on the salary of one full time employee, a commercial enterprise class firewall, installation and configuration costs plus tech support and upgrades).

However, that does not include twenty-four hour monitoring. Twenty-four hour monitoring requires at least four staff members (one for each eight-hour shift plus one spare in case of illness/vacation), which can add an additional one hundred and eighty thousand ($180,000) to three hundred thousand ($300,000) a year (not including training or benefits). With-out extra staff you cannot achieve real 24/7 monitoring and support. Assigning it as an extra duty to night staff is not an effective solution. Monitoring should be done by trained knowledgeable engineers, not with automated scripts that relay to pagers for notification.

With the number of Internet sites growing, the pool of available staff with senior level experience (five years or more) is depleted which makes personnel for such positions difficult to find much less retain. In high-tech areas there is sufficient demand to employ all people with the requited skill sets. In

[1] You may not publish these works in any medium (magazines, newsletters, zines, etc.) without the authors express permission

©Copyright Peter shipley