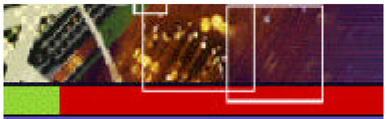

August 7, 2001

Managing IT Security Risks (Build, Buy, or Both?)

Colorado Office
1600 Stout Street
Suite 1510
Denver, CO 80202
303.446.0001

Oklahoma Office
1307 South Boulder Avenue
Suite 120
Tulsa, OK 74119
918.382.0007

Texas Office
2605 Sagebrush Drive
Suite 220
Flower Mound, TX 75028
972.899.0086

www.telechoice.com

MH389008

Prepared By:

The Strategic Catalyst™
TeleChoice
for the Telecom Industry

Managing IT Security Risks

Today's and, more importantly, tomorrow's successful enterprise is seeking ways to embrace and leverage, as well as protect itself from the increasingly agile and aggressive market environment in which it must compete. Nowhere is technology change as swift, implementation requirements as unique, and missteps as costly as they are in the IT security space.

For a majority of enterprises, securing the corporate infrastructure is a daunting task and requires specialized expertise not easily found. Keeping pace with the changing market requirements and evolving IT security technologies while also managing current shortages in available capital dollars can be difficult for nearly every enterprise. Enterprises must be selective with what they choose to protect their IT infrastructure and systems, with major focus applied to how quickly they can balance the deployment of top-notch security against softening IT budgets and profitability.

Given the rising level of risk in today's environment, security requirements are expected to quickly expand and evolve beyond today's IP VPN and firewall solutions. Many enterprises are already evaluating the features and benefits of more enhanced security solutions such as intrusion detection, virus protection, content/URL filtering, vulnerability scanning, and enhanced security reporting.

IT managers have also increasingly found themselves in the uncomfortable position of being squeezed between three uncompromising forces: lower budgets, demands from upper management to defend departmental ROI, and rising security risks. These factors often work together in a manner that results in a less than desirable solution on one or more of the three fronts. Such situations are encouraging IT managers to begin scanning the horizon for viable alternatives.

Increasingly, these alternatives involve various degrees of outsourcing, in contrast to the traditional approach of enabling security via in-house development, system and platform deployment, and new internal staffing. Outsourcing arrangements may encompass a number of activities and services, from network design and installation support to fully integrated managed security services providing both security capabilities and network access. Outsourcing firms offering such services range from value-added resellers to managed security service providers and incumbent carriers. All seek to leverage their unique backgrounds in combination with security service expertise for the enterprise interested in outsourcing some or all of its security requirements.

Weighing heavily on the enterprise's decision regarding the management of IT security measures (i.e., "do it yourself" or outsourcing) are issues such as available budget, current level of security risk, available internal security expertise, and staffing requirements. The organization's capabilities with regard to implementation and ongoing support efforts also have a critical impact on the decision. The following sections address these paths in terms of the components or pieces to consider, the strengths and weaknesses of each, and how to determine the most likely path to success for each individual enterprise.

Do It Yourself

The typical method of managing security today is for the enterprise to design, implement, and manage the solution in-house. The obvious benefits of such an approach for the end user include complete control over the finer points of its own internal security, the selection of best-of-breed technologies and vendors, and tight integration with existing platforms and systems.

However, current market conditions are forcing all but a few lucky enterprises to concentrate on achieving more with less. For example, most enterprises must deal with the following:

- Face the reality of limited or softening budgets
- Manage internal fears over ever-shifting (and highly publicized) security risks
- Enhance security responsiveness with limited personnel
- Manage operating expenses down as a percentage of revenue
- Deliver increasingly complex security solutions within constraints of slowing revenues

These market realities for the enterprise have a significant impact on how it chooses to manage the security of its IT assets. Without even considering the intricacies and challenges of the technology components themselves, managing security in-house requires an all too often underestimated investment in dollars, time, and people. Some examples of these investments include:

- Capital outlay for security-related hardware, platforms, and software
- Headcount, tools, and expertise to deliver the required security assessment and policy design
- Procurement, staging, and installation of security hardware and software across a wide geographic area
- Developing security event reporting and management functionality
- Back-office integration with existing systems and platforms
- Risk associated with delayed deployment (i.e., bridging design inception and the deployment of an active, updated security solution)
- Maintenance of ongoing technology, shifts in vendor implementations, and delivery of new security tools/features/functionality as required

Fortunately, outsourcing enables both SMEs (Small-to-Medium Enterprises) and Fortune 500 companies alike to “off-load” one or more of the issues identified above. This is one of the biggest advantages to today’s security outsourcing options in that they do not require an all-or-nothing proposition. Enterprises of all sizes can pick and choose to outsource any mix of IT security responsibilities that have simply become too problematic or too costly to continue managing with in-house staff and resources.

The Value Proposition of Outsourcing

A new breed of outsourcer has emerged affording enterprises the infrastructure and tools needed to fully deploy and support managed security solutions. These players have emerged from the growing realization that security *technology* alone is not sufficient to protect valuable corporate data. Security outsourcing firms additionally seek to address the fundamental challenges of design, deployment, monitoring, and management that an increasing number of organizations face today.

From an enterprise perspective, outsourced security providers offer the flexibility to provide best-of-breed managed security solutions while eliminating many costs associated with deploying the solutions in-house. Depending upon the particular firm, an enterprise can outsource a wide range of security functionality, typically including one or more of those listed below:

Solutions/Capabilities Enabled by Outsourced Security Providers

- **CPE Procurement.** Purchase/supply of enterprise security-related equipment.
- **Network Assessment/Design.** Analysis of the enterprise's current security environment as well as future security needs from which it will develop a security policy.
- **Deployment, Installation, and Configuration.** All initial testing and configuration of a solution. Can also address installation of software, hardware, and system integration, typically nationwide in scope.
- **Remote Monitoring and Management.** Once a solution is in place, it is a key component of an MSSP's service to monitor the network 24x7 to ensure detection of breaches and response according to defined parameters.
- **Security Reporting.** Security-specific reporting available via the web.
- **Enhanced Services.** A firm can be utilized to add enhanced security measures. Examples include intrusion detection, vulnerability scans, consulting, anti-virus, filtering, and managed CPE.
- **Support Staff.** Many providers focus solely on security and, therefore, their staff is highly knowledgeable and well trained in all aspects of such products. This leaves the enterprise's IT staff available to concentrate on the core competencies of the business.

In addition to the services available through an outsourced security provider, a number of other advantages are worth mentioning. Many create opportunities for enterprises' IT departments to help improve the strength and "competitive nimbleness" of their company over slower-moving competitors.

- **Risk-Response Time.** Outsourced solutions quickly and seamlessly integrate into the existing infrastructure without the need to delay needed security measures to re-engineer or replace existing technologies. Typically, a firm can be protecting an enterprise's critical IT assets long before internally-developed security solutions are ever ready for deployment.

- **Opportunity Costs.** Partnership with an outsourcer lowers initial development and deployment costs while minimizing overall risk. Moreover, outsourced solutions can enable the addition of enhanced security solutions in the future at a much lower financial burden to the enterprise.

- **Best-of-Breed Network and Equipment.** Through a partnership with an outsourcing firm, enterprises can ensure they arm themselves with the best-of-breed network security and equipment available. By taking a vendor-independent approach, many companies can leverage existing legacy investments and provide greater flexibility in choosing a security product that best meets the needs of each individual enterprise.

- **Self-Management and Real-Time Reporting.** Many providers utilize web-based management tools that allow the enterprise to co-manage its security environment. By giving full visibility to the network, enterprises can create and edit policy logs, open trouble tickets, and view alarms.

To be clear, leveraging the partnership benefits of an outsourced solution does not necessarily equate to an “all-or-nothing” proposition for enterprises. Many enterprises may eventually wish to control and deliver the majority or all of their security functionality from internal resources. Even under these business conditions the outsourced security provider value proposition can prove attractive. For example, the outsourcer can assist the enterprise in quickly delivering cost-effective security for its IT assets and, during this time, the enterprise can address its internal learning curves. The enterprise can minimize its security risks because a solution is already in place. Over time the enterprise may choose to bring functions outsourced to a provider in-house while it may choose to continue to outsource others.

Partnering with an outsourced security provider can be a viable and attractive alternative to deploying and managing security solutions in-house. Determining what specific components to outsource versus insource is an exercise in the evaluation of business goals, organizational competencies, and the business case.

Considering the Alternatives

There are pros and cons to any decision, and security solution outsourcing versus in-house development is no different, as each comes with its own set of strengths and weaknesses. The decision process below further examines many potential benefits of outsourcing as discussed previously. At a high level, an outsourcing partnership may be the answer for those looking to quickly acquire strong, proven security solutions and expertise and to do so with limited capital investment. With the outsourced security provider's managed solution focus, an enterprise otherwise not in an ideal position to develop such solutions itself in the timeframe needed can acquire a high-quality solution with limited financial exposure.

At the same time, the enterprise's responses to the questions posed below will reveal that partnering with an outsourcing firm is not for everyone. There can be pitfalls and sacrifices with outsourcing—understanding those issues and achieving the appropriate balance is key. By owning the infrastructure and service and having complete control over its management, the enterprise itself is obviously responsible for its own end-users' experience. However, by outsourcing the organization's security solution, the outsourcing partner controls the end-users' experience to varying degrees.

How, then, does an organization begin to evaluate where it falls on the in-house to outsource continuum?

A Starting Point

In evaluating whether to deploy security solutions in-house or to outsource some or all functions to an outsourcing firm, the organization must consider a number of factors before making a decision. The following key questions, if posed internally from a business perspective and internal competency perspective, will form a guide to help a service provider determine which path to take.

The first area to consider is the business goals of the organization and how the decision to support IT security measures will affect those goals.

- **What type of budget is in place for a security solution?**

  The primary cost difference between the two alternatives will be the capital expenditure costs to design and deploy security solutions in-house versus the ongoing expenses of utilizing an outsourcing partner. Is the organization more prepared to spend capital or to take on additional expenses in its efforts to manage its security risks?

- **What are the organization's timeframes for security upgrades?**

  Designing, implementing, and rolling out a security solution in-house can be a lengthy process requiring months of planning, installation, and testing before it is ready for general deployment. Utilizing an outsourcing partner can reduce time-to-deployment considerably due to the primary hurdles, which are contract issues between the two organizations and back-office matters rather than the deployment of hardware, software, etc. The question becomes what effect will a lengthy rollout have on the organization's protection against security risks?

- **Where does the primary business focus of the organization lie?**

  If expertise and focus lie somewhere other than in security technologies, an outsourcing partnership allows an enterprise to redirect its IT resources towards leveraging and expanding its own core competencies. The question is, are IT security solutions a complex but necessary function of an enterprise's IT department, or a major focus of the organization's value proposition in the way it conducts its business? The former lends itself to an outsourcing model while the latter likely requires the complete control of an in-house deployment.

- **Does the enterprise require sophisticated security needs?**

  This category would not only include larger enterprises requiring scalability and flexibility but also SMEs with robust security requirements, as the size of an enterprise is not always an indicator of security requirements.

  Enterprises need to ask these questions: If security is a focus, would it trust utilizing a third party for the majority of its solution? It is possible that it would not; however, the outsourcing firm's laundry list of services may provide some specific features or functions that would be appropriate in a mix with an enterprise's own in-house solution. Enhanced security reporting that typically must leverage artificial intelligence engines is an example. Will the capability exist internally for real-time analysis of system logs, or would the outsourcing partner that has the tools, expertise, and ability to present the information in reports be a more appropriate avenue?

- **Does the enterprise have more general requirements for security?**

  For such an enterprise—often assumed to be an SME—the technology and service requirements may not be as broad and complex and may, therefore, lend themselves to a simpler proposition that can be accomplished in-house. A question here would more likely come from the perspective of scale. Can the IT organization scale efficiently to serve a large number of end users? If not, what are the costly elements to serving such security requirements? As an example, it is quite likely that the expense to deploy and install equipment in-house significantly drives up the price of the solution, possibly beyond budgetary reach. With the reach and scale of an outsourcing firm, can outsourcing installation and configuration present a more palatable business solution to the enterprise?

After examining the business goals and security requirements to ascertain the impact a security solution decision will have, the next area to assess is that of competencies and staffing requirements within the organization.

- **Is security expertise an existing asset available within the organization?**

  The design and deployment of a security infrastructure and its associated solution is a complex task and requires a great deal of expertise. From platform selection to infrastructure integration, enabling security solutions from owned resources requires dedicated individuals with security knowledge. Do such individuals exist in the organization? Is their time best spent on these efforts or elsewhere for the largest organizational impact? If they do not exist, can they be found? At what cost and in what timeframe? Obviously, if the answers to many of these questions are negative, then security is not a core competency of the organization.

- **Is the support infrastructure in place and at a level to manage a security solution effectively?**

  The knowledge level and tools required to effectively manage end users once a solution is in place are very different from those of a voice or data transport solution. Security expertise will be required from end-user support to CPE configuration/installation to network management and monitoring. Does the existing support staff have the resources to support an enhanced security solution? Can it scale over time assuming success and future growth in the company? If so, does the staff have the expertise to do so and/or can they be trained? If not, does the budget exist to hire them?

Obviously, this is a short version of the more thorough organizational assessment that must be undertaken in making a build versus buy decision (or even a little of both), but it does present the foundation of the key areas an enterprise must consider. To emphasize the point again, the answer to the question of in-house versus outsource will not likely be black and white, nor will it even be a potential consideration for all enterprises. Outsourcing firms can provide the flexibility not otherwise available internally to some enterprises by delivering the critical components of the security solution needed to complement existing IT systems and infrastructures. This flexibility will give some enterprises who might not be able to fully and/or expeditiously manage security risks a solid fighting chance.

Summary

As today's marketplace changes rapidly, much of the ongoing success of enterprises' IT departments rests on their ability to proactively guard their organizations against increasingly aggressive and ever-shifting security threats. To stay ahead of such threats, enterprises must strategically arm themselves with a combination of new and existing technologies as well as experienced partners to help maximize bottom-line impact while minimizing exposure to growing security risks. A key enabler in this strategy may be the partnership of a managed security provider. With the knowledge, infrastructure, and expertise to effectively and efficiently deliver some or all of the managed security solutions demanded, an outsourced security provider can become the key or background component of an enterprise's overall solution. Offering an alternative for consideration, these outsourcers deliver to an enterprise a full spectrum of choices in building, buying, or mixing sophisticated security solutions in a way that is timely, cost-effective, and most importantly, secure.