IDC OPINION

Building a security infrastructure is a constant exercise in revision. Externally, these revisions are driven by a tightly organized, well-funded, and highly intelligent criminal element that is highly focused on specific targets. Regulatory compliance is a worldwide issue that requires accurate oversight. Internal threats are also an issue as authorized account holders (e.g., employees, customers, partners, and suppliers) engage in behavior that ranges from mischievous to malicious. Detecting and managing these incidents and events requires a hybrid approach that incorporates security products, managed services, and professional services.

SITUATION OVERVIEW

What Are Customers' Priorities?

Customers focus on the following critical tasks to help reduce security risks:

- **Anticipate** security issues that may disrupt business operations by:
  - Identifying critical assets, applications, and business operations that are crucial to corporate cash flow, profitability, customer satisfaction, and investor confidence.
  - Reconciling the criticality of the asset versus the seriousness of a vulnerability to prioritize corrective actions.
  - Establishing and reporting on compliance with internal policies and external regulations.
  - Managing the complexity (and rationalizing the conflicting priorities) of corporate business security, IT security, compliance, and legal departments.
  - Demonstrating "due care" in log management to respond to forensic and legal requests.
  - Avoiding single points of failure in security risk management by trusting just one IT organization, a single product, one professional services organization, or a single managed security service.
Remediate security incidents and events quickly and accurately with policies that ensure policy compliance and minimize business disruptions:

- Defending against the new threat environment is an increasing challenge because criminals are well organized and are working overtime to steal your data. This raises an interesting question, "Are you working harder than the criminals to protect yourself?"

- Justifying the cost of multiple security solutions to avoid single points of failure.

Investigate security incidents thoroughly:

- Quickly responding to legal requests.

- Incorporating forensic results and audit recommendations into new policies to document corrective actions, create new policies, and prevent recurrence of similar events.

Senior Management Versus IT: Friction and Resolution

Management perception can often create conflict between senior management (i.e., chief executive officers, chief financial officers, chief information officers), business unit leaders, and IT. Senior management and business unit leaders see security as a black hole from a budget standpoint, but regulatory compliance forces them to begrudgingly recognize security's importance. For senior management, compliance violations can lead to dismissal and/or public humiliation. Moreover, they recognize that security failures can disrupt critical business operations for days, weeks, months, or even years when the breach is large and the press or, worse, government agencies decide to investigate. Most companies consider even a few hours of downtime to be intolerable.

Surprisingly, the recognition of these problems is not really the source of friction between IT and senior management. IT organizations recognize these problems and are sympathetic to this pain because they know that the burden of remediation (and in some cases, the blame) will fall squarely on them. However, the perception of time and success creates immense IT frustration. Senior management (and business unit leaders) wants instant compliance, zero business disruptions, nondisruptive policies, and negative growth in IT budgets. Falling on deaf ears are IT's efforts to explain that building resilient, extensible security and compliance infrastructure takes years and millions of dollars. Ironically, it sometimes takes a catastrophic security breach to elucidate this point. Many members of senior management also don't realize that improvements in compliance don't always correlate to improvements in security.

Contributing to the frustration is the lack of recognition for IT's successes and senior management's growing distrust of IT organizations. Over the past two to three years, many IT organizations worked hard to reduce compliance violations. However, senior management simply dismissed these accomplishments as, "IT just did its job," despite IT's extraordinary efforts. In some cases, senior management even saw IT's improved oversight of compliance as a source of paranoia. With IT having vast
powers of oversight, senior management worries about IT having access to highly sensitive information. In other words, senior management wonders who watches the watchers (or IT departments), especially since an alarming number of data leakages (over 70% by some measures) derive from personnel gaffes.

Common Points of Agreement

However, some common points of agreement exist between senior management and IT. They both want an overview of their organizations’ current risk profiles. They want that view to apprise them of regulatory compliance status, critical vulnerabilities, risk profiles for key assets, and potential business disruptions due to security issues.

In other words, they both want a single source of coherent information that provides multiple layers of granularity for current and future situations. Senior management and IT agree that consolidated consoles (also know as dashboards) must encompass trends such as:

- The widening division between operational IT security and strategic security as networking diversifies into application security
- Systems management converging with desktop management and help desk
- Storage management recognizing responsibilities for securing logs, archives, and laptop/desktop files
- Security policies that encompass auditing
- Security professionals getting more involved in setting policy and reducing and managing risk

WHAT IS A SECURITY HYBRID?

Addressing these security risks requires a flexible approach that IDC calls a security hybrid. This approach combines several security mechanisms to yield a resilient security solution. Hybrid security is built on the triumvirate of professional services, security products, and managed security services. Because security risk constantly changes, hybrid security is based on flexibility. Smaller companies may require one-time professional services to write and automate policies, managed security services for monitoring and enforcement, and security products to provide internal monitoring capabilities. However, very large companies may want a greater emphasis on security products, considerable professional services (on an ongoing basis), and only a few managed security services for branch sites and/or backup monitoring. To highlight this flexibility, this White Paper concentrates on security information and event management (SIEM) to illustrate hybrid security’s flexible approach to risk reduction.
As a result, a hybrid solution contains a dynamic mix of products (hardware and software), managed services, and professional services/consulting. We emphasize "dynamic" because customers and their compliance requirements vary widely by size, expertise, budget, network topology, geographic range, and management sensitivity to security.

As shown in Figure 1, three major security components work in concert to support these processes:

- **Products.** Often, but not necessarily, the first line of customer defense is made up of the security hardware/appliances and software that the customer already owns. Because management awareness and IT expertise can vary widely, security management styles can vary widely. The nature of relationships between senior management, IT, business units, and other departments (e.g., legal, human resources, and compliance) may range from collaborative to wariness to outright hostility. Sometimes, these groups exercise ownership rights over certain assets, making collaboration even more difficult. In some cases, however, this ownership (at the corporate and/or departmental level) is mandated by government and industry regulations.

- **Managed services.** To supplement overburdened IT organizations and/or provide a second source of analysis, customers utilize managed services to correlate internal scans and external vulnerability monitoring. Often, these services can provide an early warning of an impending threat. Intrusion detection services can also supplement internal efforts by remotely configuring systems, automating updates/upgrades, consolidating software support, and offering higher-level analysis. For midsize companies, customers can use managed services to avoid increases in operational budgets for more personnel and capital budgets for new security products. For enterprises, customers can get a second opinion on developing threats, remediation, and forensics. Managed services can also provide a deeper level of analysis than internal groups. For example, some customers probe compliance issues because they want to maintain a consistent level of compliance versus past situations in which compliance was maintained only for the month of the audit.

Overall, managed services provide the expertise to enhance security information management tools. Managed services can address customer issues concerning the expertise or resources needed to monitor on a 24 x 7 basis. They can provide second and third shift monitoring when expertise is present but resources are limited. When expertise is limited or completely lacking, managed services can take over all monitoring.

In either case, managed services provide an external view that can help deal with sensitive questions such as:

- Are members of your IT organization compromised?
- Can you trust IT to do the monitoring?
Can you go beyond the in-house expertise for 24 x 7 monitoring because of budget constraints, limited expertise, or lower priority of second and third shift monitoring?

Can you correlate internal, external, industry, and global issues?

How should you prioritize your response?

Can you track and audit all elements of the response and remediation process?

**Professional services.** As we pointed out, products and managed services can work in concert to reduce risk, improve compliance, and even lower capital and operational costs. However, managed services are not designed to deal with an individual customer’s in-depth questions about its specific issues. This is where professional services are needed.

**FIGURE 1**

Hybrid Security Model

Source: IDC, 2007
Customers use managed services to maintain a consistent level of compliance throughout the year, but professional services design the process for easy maintenance by managed services. Additionally, professional services design, implement, and (in specialized cases) maintain customized security solutions. To develop these customized processes, external consultants can help customers with incident planning, incident response, penetration testing, forensics, and other services. In most cases, consultants remain onsite only for a short time. In other cases, midsize and enterprise businesses may employ a part- or full-time consultant to administer security systems, manage strategic projects that are beyond the IT department's expertise and/or workload, act upon recommendations provided by the computer incident response team (CIRT) and managed service solutions, or even take on responsibility for executive management of security operations.

**Processes for Hybrid Solutions**

When building a hybrid solution, companies should look at some basic requirements. Security risk management should start with consideration of the following important processes:

- **Assessment and planning.** Professional services often take the lead in consulting on the initial assessment, analysis of critical issues, prioritization of information assets, developing a strategic plan, and constructing solutions and management groups. After the consulting phase, professional services work with IT and senior management to fix tactical issues and build a strategic platform that provides a structured incident response while reducing the incidence and severity of future threats.

- **Log consolidation.** This function aggregates logs from a heterogeneous mix of intrusion detection/prevention systems, identity management solutions, firewalls, antivirus solutions, vulnerability managers, databases, operating environments, routers, switches, and virtual private networks. To supplement customers' lack of log management resources, managed security services focus on threat management technologies (e.g., firewalls, intrusion detection/prevention systems, and malicious code) with alerting for full context on the incident.

- **Event management.** This function normalizes logs, assesses vulnerabilities, and inspects data for policy compliance violations. It can consolidate logs from heterogeneous systems to provide an overall view of the event. Third-party intelligence services that provide global information on new threats are highly valuable as external supplements to internal event management systems.

- **Security information management (SIM).** This function correlates event management output and external scans, correlates to detect attacks, prioritizes incidents based on criticality of assets, and provides a workflow process for handling situations.
**Incident response management.** Even the best laid plans will not proactively mitigate all attacks. Therefore, incident response management is needed to deal with attacks such as denial of service, malicious code, new (and old) exploits against unknown vulnerabilities, and internal security issues. Most customers already have their own version of CIRT, but these internal groups can be bolstered as follows:

- Consulting services that backstop internal organizations can provide a global view of the problem and the possible solutions. By tailoring a program to their unique needs, customers can choose a flexible approach that enables them to manage the CIRT in conjunction with onsite consultants and/or a managed service.

- Full-cycle approaches to CIRT are important. The combination of products, consulting, and managed services should contain all these elements: process for escalating incidents, suggestions for remediating the problems, recovery mechanisms (systems, applications, and data), investigation of the root cause, review of the incidents, and recommendation of preventative actions.

**Scenarios for Mixing SIM, Managed Services, and Consulting**

Mixing SIM, managed services, and professional services offers many flexible opportunities for distributing workloads, handling shift work, and providing deeper analysis. A hybrid approach that uses professional services to integrate SIM, managed services, and consulting can efficiently support different network taxonomies and customer sizes. A hybrid approach can enable customers to compromise on difficult issues such as budgets (capital versus operational), security expertise (internal versus external), daily monitoring (single versus second or third shift), and geographical coverage (security staff in one country versus a few major countries versus everywhere). With customized professional services, customers can have a virtual dial that determines the degree of internal support versus external support.

**SIM Products and Managed Services for a Distributed Topology**

In this scenario, branch SIM modules forward data to a centralized SIM module and a managed service for further analysis. Customers derive value from the managed service's second opinion and an early warning on global threats. Professional services are used on an irregular basis for analyzing critical incidents and doing forensics.

**Managed Services for Off-Hours Monitoring and Secondary Analysis**

Another scenario might forward data to an internal SIM module for in-house analysis during normal business hours, but the customer uses managed services during off-hours. This customer benefits from second and third shift monitoring without the additional staffing overhead. Professional services are used to analyze newly acquired companies and integrate them into this environment.
Multistage Analysis with Products, Managed Services, and Professional Services

In this scenario, customers demand a very high level of analysis because of their low tolerance for security risks. To accomplish this goal, the centralized SIM module ships data to onsite consultants in a CIRT capacity. They consolidate the data from both the SIM modules and the external managed services. The aggregate data is presented on a dashboard to standardize incident response and remediation.

Compliance Monitoring

When it is not efficient to send all logs for all systems to a central site, SIM modules can search for compliance violations at the local site and pass violations to a central site. This sharply limits traffic to the central site and reduces analysis needs. Professional services can help monitor regulatory compliance and suggest remediation strategies. With this option, customers have a flexible solution that can scale to appropriate levels of log information. To accommodate regulatory changes, consultants’ expertise enables customers to fine-tune their compliance infrastructure on a regular basis.

Crisis Management

A crisis can also precipitate the need for managed services. A customer may need instant remediation capabilities to avoid further scrutiny, exposure, fines, and ongoing audits. In some cases, legal issues or compliance problems may mandate continuous auditing. Given the limited time and resources that most companies have, a managed service may be a necessity. Professional services may also be necessary to perform the onsite remediation to deal with the immediate problem. After the crisis, these consultants may participate in forensics and policy revisions to prevent a reoccurrence.

Dual-Stage Monitoring for Risk and Cost Reduction

To reduce risk and avoid the cost of hiring high-level analysts, some customers do high-risk system monitoring with a managed service for 24 x 7 coverage while low-risk system monitoring goes to a SIM product. This dual stage offers a substantial element of "risk management" because this process evaluates risk and implements different controls based on risk profiles. Professional services are often invaluable in determining risk levels and the criticality of assets so they can be segregated in the dual-stage scenario.

Managing Log Retention

Log retention is another area in which SIM and managed security services work well together. SIM provides a guaranteed log data store for the desired period, whereas managed security services are more one size fits all. Consulting can provide advice about where the logs should be kept, access privileges, analysis, and retention periods.
Accommodating Mergers and Acquisitions (M&As)

Many companies grow by merging or acquiring other companies. The hybrid approach can help with M&As, due diligence, and/or consolidation of multiple networks. Managed services can handle distributed sites without increasing headcount. SIM products can provide a consolidation point for logs, incidents, and events. Professional services can consolidate security technologies, design more efficient processes for SIM, assess security vulnerability, prioritize responses, participate in the CIRT, respond to remediation guidance provided by a managed security services provider, and manage aspects of security operations.

Critical Issues

Customers should settle critical issues before looking at a specific scenario. How much analysis and reporting should remain in-house? If customers want or need (based on regulatory, industry, or internal policy) all data and analysis to remain in-house, then SIM should remain separate. If they don't want this capability, then managed services make more sense.

Most companies have internal and external auditors, so some customers might want external managed services to validate internal SIM results and check one against the other. IDC estimates that customer spending on SIEM will increase at a 25.2% compound annual growth rate from 2006 to 2011 (see Figure 2).

Figure 2


Source: IDC, 2007
However, IDC is hearing from more customers that they want more flexibility than just SIM or SIEM (IDC’s term). They want SIM for low-priority risks and the flexibility to run managed services against a high-priority asset. Or, they might want an external scan when new vulnerabilities and attacks are known or suspected.

Another major question is, How critical is SIM expertise to customers? Many smaller companies don’t want to invest in this expertise, but they still need reports on incidents and compliance. Managed services may be a significant alternative for these customers. Other companies may want to employ a consultant to monitor their SIM product from an onsite location. Customers will have easy access to a dedicated resource with a high level of expertise, but the firm does not add headcount.

**Consolidated Console**

To build a consolidated console, companies should consider the processes mentioned earlier (log consolidation, event management, security information management, and incident response management) as a set of shims that integrate into one dashboard or authoritative source of information. While customers may want to build this dashboard in-house, IDC believes that larger enterprises should seek assistance from professional services in building and operating this dashboard. Their expertise, particularly when analyzing logs from SIM products and managed services, is the key to building a knowledgeable and responsive CIRT team.

**Roles for SIM, Managed Services, and Professional Services**

Misunderstanding the roles of SIM and managed services is a significant issue that can endanger the hybrid approach. The role of SIM is not detection but correlation of anomalous activity to prioritize remediation — without human analysis.

As shown in Figure 3, some customers think that SIM contains instant remediation capabilities. In fact, SIM does not auto-delete users, clean viruses, or change firewall rules; rather, it provides IT with steps to remediate. For example, when a new trojan is detected by the antivirus or vulnerability management (VM) solution, SIM explains how it impacts the customer’s environments and what vulnerabilities it exploits.
A managed service also does this, but typically for only a subset of data and without flexibility. However, managed services usually add a layer of human expert analysis. Customers typically have their own vulnerability management with scanners in different parts of the network.

A SIM product does an intelligent analysis of these scans, prioritizes the results based on the criticality of assets, and offers suggestions on remediation. A managed service, however, can include vulnerability scanning services for a more complete solution.

Onsite consultants take this a step further by putting the data in the context of the customer's business. SIM products and managed services offer limited remediation recommendations, but many customers will need human analysis and validation versus automated correlation. Specifically, consultants are needed to design the process for escalating incidents, remediating complex problems in a highly customized environment, building recovery mechanisms for heterogeneous networks, investigating the root cause, managing a corporatwide review of critical incidents, and creating preventative measures.

**Hybrid Concept Caveats**

In large and/or distributed environments, lower-cost event management products can collect logs, distill them, and pass them on to a managed service. A hybrid concept provides an interesting alternative by doing some SIM analysis on premises and other
analysis at the managed service (i.e., bug view). This sounds good, but it can't be done efficiently with two independent tools. The hybrid concept needs full integration between the two systems. This means similar reporting, information passback, and integrated portals for information retrieval. Customers are aware that SIM is maturing, but because older products can't handle the volume and provide poor reporting, achieving the hybrid concept may require newer SIM products and more current managed services offerings. IDC notes that this functionality is not on many vendors’ current managed services and SIM integration road maps. Customers should be aware of this limitation and use professional services to bridge this gap.

**Patch Management Integration with SIM**

As for integration with patch management, most SIM and managed services offer Web services application programming interfaces (APIs) that interface with patch management systems. Some customers use a programmatic approach to kicking off the patching process when critical vulnerabilities arise. However, most enterprises are loath to automatically invoke patching without prior testing of patches. In some cases, untested patches can cause more harm than good because of customers' highly customized environments and variability in patch quality.

IDC thinks this is another critical issue. In some cases, the SIM product and the managed service will tell the customer different things. Also, these recommendations may not be relevant to the customer's business goals. By analyzing business objectives, prioritizing assets, and correlating recommendations from the SIM product and managed services, professional services can provide the human element that optimizes the response based on the needs of the business at a particular time.

**Compliance and Privacy Issues When SIM and Managed Services Work Together**

For many customers, compliance and privacy are big issues when it comes to a hybrid approach. Customers that have succeeded in this area made sure they received satisfactory responses to the following issues:

- **Data privacy** when SIM data is passed to managed services and/or centralized SIM modules
- **Data leakage** when information is analyzed by unknown analysts at managed services and/or professional services firms

Some hybrid customers have implemented anonymous cleansing of customer data so that local SIM does not pass any confidential customer data to the managed service. In this scenario, the SIM product does heavy analysis and passes only metadata back to the managed service for greater analysis.

Where government regulations prohibit the exporting of customer or consumer data, this approach can reduce or eliminate the need for a local security operations center (SOC) in each country.
**PCI DSS and SOX Compliance**

Compliance with specific regulations raises other issues. Payment Card Industry Data Security Standard (PCI DSS) is a big issue for customers that accept or process payment cards. PCI DSS requires customers to save one year of logs. The Sarbanes-Oxley Act of 2002 (SOX) requires seven years of logs. The process of searching, storing, and retrieving so many logs is expensive and difficult. Customers are beginning to adopt archive management systems that work with forensics, but they are realizing that the logs must be safe from change, easily retrieved, and available for correlation analysis (e.g., failed log-in attempts coupled with firewall failure).

Good forensic support is critical, but most customers want to avoid the need for this activity by taking positive steps well in advance to reduce the potential for a crisis. To do this, they regularly run reports for auditors, security people, and senior management. These internal reports are compared with results from managed services. In best-practice situations, these reports hopefully show improvement over time for IT and senior management.

For IT, the reports document its achievements and managed services provide independent corroboration. For senior management, the reports highlight gains from the previous audit, remaining areas of weaknesses, and the length of compliance. (Increasingly auditors are looking for consistent compliance levels over time, not just for a few weeks preceding and following the audit.) Some managed services can even provide competitive comparisons so that customers can corroborate their efforts against those of other financial services companies.

**Customer Stories**

This section profiles some early hybrid implementations. All customers are anonymous and some details have been changed to protect confidentiality. Most customers started from the SIM side and then went to managed services to avoid overstaffing. IDC estimates that roughly 20–30 financial services firms have made this expansion. Driven by new NERC/FERC regulations, some energy companies are also adopting hybrid approaches. Likewise, big retailers are also considering this implementation because of PCI DSS. They recognize that doing their own correlation and aggregation is too costly and prone to internal errors and other issues.

Because every customer has some manual log analysis, event management, or SIM functionality currently installed, there are no "green fields." Still, customers are dissatisfied with these "islands" of compliance and security. They are under pressure to look at the whole map. Many customers examine their most vulnerable islands with a managed service and some rudimentary analysis with manual data collection once a year to pass the audit.

Customers want to add SIM integration for internal compliance and log management. Some companies with their own SOC or network operations center (NOC) are attracted to the potential cost savings of a managed service. Some organizations (especially government defense departments) are funding multilayered, granular data analysis. In this scenario, they use internal SIM modules at a distributed site to do log correlation and coarse-grained aggregation. Internal, centralized SIM modules do
finer-grained analysis and reconcile with internal and external regulatory compliance policies. Managed services are used for finer-grained analysis and corroboration. For deep, custom analysis, customers are relying on professional services. In some cases, consultants work offsite on custom data sets, policy enforcement, remediation, and forensics. In other cases, they work onsite for a few days to a few weeks, providing a high level of analysis or working for senior management on an IT-independent assessment. In a few cases, large companies and even some midtier companies employ full-time personnel from professional services firms in lieu of advanced IT personnel.

Overall, there is some frustration among the early adopters because many hybrid implementers have disparate systems that they can't aggregate and correlate. Political issues have also hampered progress. Senior management doesn't understand the economics of hybrid approaches. IT organizations argue that they don't need a second opinion, and they worry about increased oversight and possible outsourcing. As previously mentioned, government-mandated customer privacy issues may require in-country SOCs.

**Government Contractor: Addressing Annual Compliance Decay**

For many companies, compliance is a constant battle. The problem is that many companies are out of compliance for 10–11 months a year. For one month every year, this financial services firm allocated roughly one-quarter of its entire IT staff to prepare for the regularly scheduled, annual audit. It had separate SOX, Health Insurance Portability and Accountability (HIPAA), and Federal Information Security Management Act of 2002 (FISMA) teams. The audit team also pulled in the accounting department for help with accounts receivable (AR) because only the AR analysts understood where the general ledger was located in the database.

Every year after the auditors left, the system decayed and the contractor gradually slid out of compliance. The CEO hated this decay. She wanted an automated status system because she worried about unannounced and random auditor visits. The CEO and IT shared a common desire for a comprehensive compliance dashboard. Recognizing that 100% compliance was impossible because of a constantly evolving IT organization, both groups wanted a dashboard that would provide a near-real-time view with an emphasis on critical situations.

To eliminate this annual cycle of compliance and noncompliance, the contractor automated the manual process of log aggregation, installed centralized SIM appliances to report on the state of compliance, and employed managed services on an irregular basis for an independent assessment. Irregular analysis was a specific action to simulate and prepare for future unannounced audits. Professional services were also employed for a few months to reconcile conflicts between IT and the CEO, build new compliance processes, and integrate the company's SIM appliances with managed services.

Overall, the customer is happy with the outcome. Initially, the CEO was unhappy with the time and cost despite the IT department's very accurate estimates, but this friction seems to have been resolved. As for next steps, the CEO and IT are exploring archive management.
**State Government: Improving Compliance and Forensics While Cutting Costs**

This large state government has 20 agencies, no centralized SIM capability, ongoing compliance and security issues, cost pressures, and a lack of trained personnel. It needed help with training, consulting, and even hiring onsite people to integrate the implementation of a managed service. The state also wanted dedicated, external consultants to create reports and custom analysis for senior management.

Before managed and professional services, the state agencies did not have a common compliance platform. As for costs, each agency spent a total of $300,000 a year for two SIM licenses (roughly $150,000 a year) and one onsite full-time equivalent (FTE) ($150,000 a year). Multiplied by 20 agencies, the state spent $6 million a year on security-related compliance and employed 20 FTEs. Compliance was problematic and security incidents were regular events because some agencies lacked trained personnel; therefore, no one was available to look at logs when an incident occurred. IT constantly struggled with the dilemma of pulling an IT person off a production job for a couple of weeks to meet legal requirements.

After the state brought in managed and professional services, costs fell. More importantly, compliance reporting improved enormously. Managed services cost $250,000 a year per agency. For 20 agencies, the cost totaled $5 million a year. This does not include eight centralized FTEs for analysis and policy recommendations. Three internal employees remain dedicated to SIM at a cost of $450,000 a year, and the two permanent onsite consultants cost $400,000 a year. This brings the total to $5.85 million a year.

(Please note that all cost calculations are approximations and individual figures have been changed at the customer's request. Costs will vary sharply by customer location, size, industry, compliance environment, and preexisting conditions. Caveat emptor.)

A savings of $150,000 a year seems pretty marginal, but the state government feels that improving security while reducing costs is a very large win. The state still has SIM expertise with its own staff, managed services for third-party corroboration of the state's analysis, and onsite professional services to provide a deeper level of granular compliance enforcement and handle shifting problems. The state believes that this hybrid solution provides a greater depth of analysis, reduces costs, increases responsiveness, increases security, improves its crisis response, and helps it respond to constituent issues on a more timely basis.

---

**Conclusion: Customers' Suggestions for Qualifying Vendors of Blended Solutions**

When customers were informally asked about qualifying vendors of hybrid solutions, they responded with the following comments:

- **Vendor understands, supports, and meets present and future needs.** This is not just at the technical level, but at the business level as well. I need to feel that the product and vendor fit with my future IT strategy, or even that the vendor can help me shape my future IT strategy. This requires that the vendor understands my business needs.
- **Technically sound.** The product meets all my current and anticipated technical requirements. The vendor can guarantee a reasonable level of service, in terms of both the product and support.

- **No labor issue.** My existing staff understands or can easily assimilate these products and services. If I need to hire additional staff or replace staff, I will readily find what I need in a managed or professional service so the implementation process will not be overly long or expensive. This means that the integration between installed products, in-house expertise, and external service should not be obscure. There should be a ready supply of competent people to support it. Furthermore, I can bring in high-level consultants for specialized tasks (one a one-time basis) that are too sensitive for IT and/or beyond their technical capabilities. These consultants may also facilitate the more rapid delivery of IT-based solutions by resolving conflicts, technological obstacles, and political conflicts.

- **Vendor viability.** The vendor is in it for the long haul; they are not likely to be acquired and have this technology become deemphasized or its service level downgraded, and I won't be forced to convert to something else.

- **No strings.** This solution does not require me to acquire technology. I would not acquire or enter into a commercial relationship with a vendor with which I would not otherwise do business. It has few or no dependencies on other products that could go away or slip out of support, and it does not "lock me in" to a technology (platform, OS, middleware, etc.) that I would not otherwise commit to long term. This also implies a requirement of support for open interface standards and architectures or a requirement for interfaces and architectures so ubiquitous as to be de facto standards (such as those of the Windows platform).

---

**Copyright Notice**

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2007 IDC. Reproduction without written permission is completely forbidden.