



Understanding the value of outsourcing network security services



EXECUTIVE SUMMARY

The enterprise network has never been more difficult to secure. Networks are more complex, with more endpoints, connections, applications and data to monitor. Threats are more sophisticated, and there are more forms of threats and more security breaches than ever before. There are new regulations to address. And while mobility returns many strategic benefits for the enterprise, the use of wireless LANs (WLANs) and wireless WANs (WWANs) creates constantly changing network perimeters and new challenges not found in the world of wired networks. And if a breach does occur, the financial impact can be devastating.

Two activities are core in helping enterprises address network security. The first is a thorough assessment of your network today to uncover and address any existing vulnerabilities. The second is the day-to-day 24x7x365 monitoring of the network for security incidents — from rogue access points joining your wireless LAN to the loss of a mobile computer with highly sensitive company data or the introduction of a virus into the network.

How can you best uncover and address the security vulnerabilities in your enterprise network? And how can you best secure a network that is constantly changing and continually exposed to new threats? Are your security needs best served by an in-house IT department — or should you consider outsourcing? And if you determine that outsourcing is right for your company, what do you need to know to help you select the right vendor for these truly mission critical tasks?

This white paper will examine the many new challenges that are facing today's network owners, the pros and cons of using in-house resources and outsourcing for your network assessment and day-to-day monitoring, as well as guidelines to help select and maximize the value of outside resources.

New challenges increase the complexity of securing today's enterprise networks

New technology and new trends in the business world have led to the increasing complexity of corporate networks. No longer confined to wired connections inside the enterprise walls and between enterprise locations, today's networks must be able to provide a virtual extension of the enterprise to practically any corner of the world to ensure critical voice and data access for many types of workers — from service and sales teams who spend their day in the field to traveling executives, telecommuters and more.

As a result, there are more networks to monitor and secure. In addition to the local area network (LAN) and the wide area network (WAN), there are wireless LANs (WLANs) as well as a wireless wide area network (WWAN) that may include a number of public cellular carriers.

There are more devices — end points — to secure. In addition to desktops, there are laptops that routinely leave the building every day, as well as handheld mobile computers, personal digital assistants (PDAs), mobile phones, web servers and access to many line of business applications. And mobile devices present a unique challenge — a constantly changing network perimeter.

There is a higher volume of data to secure. In addition to the large amounts of data stored on mobile and wired devices and servers, data is moving through the air all day long, in transit to and from mobile devices inside and outside the four walls.

And there are more connections to secure. In addition to connections to your employees at work, home and on the road, you now also likely extend connectivity for certain business applications to customers, vendors and other partners to improve productivity and customer service levels.

While the number of entry points into the corporate network has increased, so has the threat of unauthorized network access. Today's attackers are no longer just hobbyists, but now include professionals who are constantly developing new

cyber attacks and searching for network weaknesses to gain access to company data, attested to by the sharp rise in the number of security breaches. In the U.S. alone, the San Diego-based Identity Resource Center estimates that approximately 79 million records were exposed in 2007 — four times the estimated 20 million lost records in 2006.¹

With so much personal information now stored on computers, breaches no longer threaten only the enterprise, but the enterprise customers as well. New regulations have been created to help protect highly sensitive client data. For example, the Health Insurance Privacy and Accountability Act (HIPAA) helps ensure the safekeeping of patient data in the healthcare industry. And Payment Card Industry (PCI) regulations provide mandates to retailers to protect consumer credit card information. To further compound security challenges, in addition to their own internal security policies, healthcare organizations and retailers must also comply and provide proof of compliance with these regulations.

The devastating cost of a data breach

Today, virtually all critical data is stored electronically. As a result, there is more at stake from a security breach than ever before — damages can include fines, sanctions, penalties and even lawsuits. For example, retailers who are non-compliant with PCI mandates can lose credit card processing privileges — a catastrophic event for a retailer. In addition, banks can — and have — sued retailers for losses associated with a data breach. And power utilities can face million dollar fines per day per violation.

When customer data is stolen, the cost of a single breach can reach astronomical heights that can easily threaten the health of your business. There is the physical cost of the lost record, estimated at \$90 to \$305 by Forrester Research.² There is brand damage and the impact on customer loyalty — Javelin Strategy & Research reported that 77 percent of 2,750 consumers polled stated that they would stop shopping at stores where data breaches had occurred.³ There are legal liabilities for affected customers — for example, 1,800 cases of fraud have been linked to a supermarket chain breach that exposed 4.2 million credit and debit card numbers.⁴ And there is the high cost of the daily disruption of business. While competitors are focused on improving and growing their businesses, many workers in the enterprise will need to concentrate on

“77% of 2,750 consumers polled said they would stop shopping at stores that suffer data breaches.” and “...85% will reward merchants that are perceived as security leaders by giving them more of their business”

Three of Four Say They Will Stop Shopping at Stores that Suffer Data Breaches;
Information Week; Sharon Gaudin; April 12, 2007

the ‘cleanup’ effort, which can result in staggering productivity losses. For example, IT staff must determine how the breach occurred and take appropriate measures to increase security, while administrative personnel are calling customers to inform them of the breach.

Network assessment and day-to-day monitoring: in-house or outsource?

Securing the enterprise networks starts with the development of a security strategy that includes a number of basic tenets, including a thorough and regular assessment of your existing network security programs as well as day-to-day monitoring of the entire network — wired and wireless infrastructure as well as the wired and wireless devices.

Routine assessment of the entire network infrastructure as well as existing security programs — from policies and security design to incident response procedures and physical security — will help uncover existing vulnerabilities and their associated risks, allowing the enterprise to make intelligent decisions regarding the management and priority of those risks as well as the IT budget.

In addition, the network must be protected around the clock against intruders who would steal customer and company records as well as from the nuisance and disruptive actions of worms and viruses that could affect network access — and employee productivity. To secure the network, enterprises must be able to instantly spot and contain security events, suspicious activity and lost or stolen devices, requiring the 24x7x365 monitoring of firewalls, intrusion detection sensors and switches to routers, authentication servers, antivirus servers, access ports and points, mobile devices and more.

These critical pieces of your security program can be executed by your in-house IT team or by an outside resource — such as a Managed Security Service

Provider (MSSP) for day-to-day monitoring. How can you determine which choice will best serve your enterprise? To answer this question, you need to evaluate a multitude of criteria for each approach, including the quality of service, cost, scalability, risk and control.

Service quality

To assess the quality of service — in house or outsourced — you need to examine the level of expertise of the workers who will be actively involved in either assessing or monitoring your network, the types of processes that will be implemented and how consistent and rapid the response times will be to any security incident.

Breadth and depth of security expertise

In order to best protect your network, administrators should possess the highest level of expertise possible. Many in-house Security Administrators are concerned primarily with password management, firewall monitoring, addressing email spam and eradicating viruses. But today’s security experts need to be well versed in spyware, intrusion detection and prevention, phishing, web scams, identity management, compliance reporting and patch management — as well as any new type of threats that today’s sophisticated hackers might invent. Outsourcing data security management to an expert MSSP provides a distinct advantage in this area. If you consider the world beyond the network perimeter as potential ‘enemy territory’, MSSPs are on the front lines. Constantly monitoring many networks with many locations every minute of every day, they are usually the first group to spot and determine how to neutralize new threats. When you hire an MSSP to secure your network, you gain access to this extremely rich security knowledge base, providing the highest level of proactive security for your enterprise network.

Mature best practices

Since MSSPs are key partners in security programs at many companies, they can offer an advantage: knowledge of standard security best practices and requirements for your particular industry. This allows

the MSSP to deploy mature, fully developed and fully tested security practices in your enterprise right from the very beginning of the engagement. This knowledge proves invaluable in planning and network assessment as well as day-to-day monitoring.

Timing

Timing is everything, and when it comes to detecting suspicious or possibly malicious activity, nothing could be more true. Businesses need to know that a security incident will receive instant attention; that it will be addressed as quickly as humanly possible. Both in-house resources and outsourced solutions may offer equivalent advantages here. Your own staff is right down the hall, able to respond promptly — provided that they have the staff, tools and training to sift through the volume of data to detect and characterize the event, determination if action is required, and if so, what appropriate remediation steps to execute. On the other hand, despite being offsite, you can count on a good MSSP to employ personnel with the right expertise, training and tools to detect, characterize and act rapidly within the response times that are clearly spelled out in your service level agreement (SLA).

Cost

Assess the capital and operational cost of both approaches to provide an understanding of the financial impact of utilizing in-house and outsourced resources, as well as the challenges associated with managing the security budget.

Capital investment

In-house security monitoring involves the selection and purchase of hardware and software to collect and store all the data, software and ongoing software updates) to view and analyze the data, as well as any other assets required to monitor the network. The enterprise must be able to justify these purchases. Alternatively, an MSSP has already made the investment in the equipment required to monitor your network, and can use economies of scale to your advantage, minimizing the upfront capital investment required for day-to-day monitoring.

Operational costs

According to Stratecast Partners, a division of Frost & Sullivan, one full time equivalent (FTE) is required for a bare minimum of security oversight for every 200 employees, at an estimated \$120,000 per year (salary and benefits) for a moderately experienced security manager.⁵ This translates into \$600,000 per year just in salaries for a company with 1,000 employees. In addition, constant security software

updates are required. The emergence of new threats translates into the need for ongoing employee training. And IT management and human resource personnel time must be factored in for hiring, staff management and management of any turnover in staff.

By comparison, since MSSPs provide all the trained manpower required, there are no annually recurring operational expenses associated with network security — no annual salaries, software updates, training or management costs. As a result, your costs are defined and predictable.

Budget management

Creating and managing your security budget requires the capture of many different types of costs related to security — from capital expenses for hardware and software to operational expenses related to annual salaries, training and management. In addition, part time or temporary employees may be needed from time to time due to unexpected illness or other unforeseen and unplanned absences. And new threats can ripple into a greater than expected need for new training, equipment and software. The volatile nature of security management and the absolute requirement for 24x7x365 coverage can result in budget exceptions.

On the other hand, outsourcing provides predictable costs that are pre-defined in the contract. Everything required is to be supplied 24x7x365 for the duration of that contract, eliminating 'surprise' purchases that exceed available budget.

Scalability and IT staff utilization

When security monitoring is handled in-house, staffing schedules need to account for vacations, ample coverage during any turnover in staff, and even additional manpower to address a major threat. As your network expands, you may need to scale up your around-the-clock monitoring capabilities — adding headcount and equipment such as security servers, routers or intrusion detection sensors.

In addition, when your internal IT staff is tasked with the day-to-day routine security monitoring of your network, their ability to focus on more strategic technology initiatives is impaired. In the event there are initiatives that require attention, the enterprise may need to expand the workforce. And the cost for these extra workers — from salaries, benefits and other infrastructure such as a computer and phone — adds to the cost associated with in-house security.

“For many enterprises today, the question should be, “Why haven’t we outsourced the day-to-day grunt work of managing security devices?” By choosing a quality MSSP, most enterprises will see an improvement in their security posture and free up internal resources to address the critical security needs of e-business.”

John Pescatore, Choosing a Managed Security Services Provider, Gartner, Inc.,
Note Number: COM-14-2210, August 31, 2001

When security monitoring is outsourced, scalability is a non-issue — the MSSP not only provides any additional manpower, equipment and facilities that are needed at no additional cost, but also manages the integration of new mobile devices, mobile applications, security policies and more in the enterprise (within the guidelines of the MSSP Service Level Agreement). Outsourcing also frees IT staff to focus on more crucial initiatives that are more strategic to the business — such as a mobile sales force automation or field service applications — keeping IT employees focused on business initiatives that help improve core competencies.

Risk

Since the enterprise does not have direct control over a security vendor, there can be a high perceived risk associated with outsourcing security — the enterprise does not control the hiring of employees, and cannot control employee integrity nor response times. We refer to this risk as perceived risk, since there is actually equal risk inside the enterprise.

Recent statistics reveal that, indeed, external sources are the cause of the majority of data breaches: 73 percent of data breaches are attributed to external sources, 18 percent to internal sources and 39 percent to partners (defined as any 3rd party sharing a business relationship with the enterprise, including vendors, suppliers, customers and contractors).^{*6}

While externally generated breaches outnumber internal breaches four to one, the median size of an insider breach (measured by the number of affected records) is 10 times greater than an external breach.⁶ While there may be more breaches from external sources, it is the small amount of internal breaches that can do the most damage. Breaches originating through partners (considered as a form of internal breach) are second in terms of magnitude, affecting on average six times the number of records typically affected by internal breaches:

Breach Type and Impact⁶

Breach Source	Number of Breaches*	Number of Affected Records
External (hackers, organized crime groups, government entities and environmental events such as typhoons and earthquakes)	73%	30,000
Internal (company executives, employees, interns and other assets such as physical facilities and information systems)	18%	375,000
Partner (any third party sharing a business relationship with the enterprise, including partners, vendors, suppliers, contractors and customers)	39%	187,500

An even more startling statistic is the breakdown of who is at the center of internal breaches. According to the Verizon study, which draws its statistics from the forensic analysis of over 500 security breaches, half of all internal breaches are attributed to the company’s own IT administrators.

Using the above numbers, out of every 100 breaches, the 73 externally based breaches affect a total average of 2.19 million records (73 incidents x 30,000 records), while the 18 internal breaches affect an average of 6.75 million records (18 incidents x 375,000), with 3.38 million (half of 6.75 million) attributable to internal IT staff.

In the 500 incidents that were analyzed, in spite of the fact that the enterprise had complete control over their IT staff, and that the number of external breaches far outweighed that of internal breaches, the number of compromised records attributable to a company’s own IT staff was 54 percent more than the total number of compromised records in all the external breaches combined.

* Note that percentages do not add up to 100 percent as over 25 percent of the cases in this study cited multiple sources.

This research reveals that the risks associated with in-house security services have the potential to have a much greater negative impact on the enterprise. Outsourcing to a carefully selected vendor can remove the majority of this threat — inside IT personnel would no longer possess the knowledge or tools to easily execute a planned security breach.

Control

When you choose to manage security with your in-house IT staff, you have complete control. You choose whom to hire and you have complete control

over your solution — from tool selection to the development of policies and standard operating procedures (SOP).

Clearly, you do not have this level of control with an outside vendor. You do not choose the employees or the tools, nor do you set policies or SOPs. However, this is offset by the fact that you are in control of the selection and management of that vendor. The relationship with a security vendor is subject to the terms of the SLA. And just as you directly control the performance of your employees, your SLA controls the performance of your vendor.

In-house vs. Outsource Score Card

As the scorecard below indicates, there are many advantages associated with outsourcing network security monitoring.

Criteria	In-house	Outsource (MSSP)
Capital Investment	Hardware, software	None
Operational Costs	Staff, Training, Management time, HR time, equipment maintenance	None
Service Quality: Expertise	Often a general and/or modest knowledge base	Broad and deep knowledgebase; specialists with deep knowledge in specific areas
Service Quality: Responsiveness	Limited knowledge, competing priorities	Expertise and automated tools; 100 percent focus on the security of your network — no competing job priorities
Service Quality: Best Practices	Limited knowledge	Expertise
Budget Management	Subject to unforeseen expenses	Known static annual costs
Scalability	Major effort to scale	Easily scalable
Control	Direct management	Indirect management
Risks	Equivalent	


 = Advantage

Outsourcing: selecting and evaluating a vendor

With such a strong business case, you may be considering outsourcing some of your security services, such as network assessment or day-to-day monitoring. Vendor selection is the most important decision you will make with regard to outsourcing security — the wrong vendor isn't likely to be able to provide the right services for your specific situation. Key criteria to assess include:

Familiarity with your industry and the technologies you use

The MSSP you choose should be able to demonstrate expertise in your industry, with knowledge of best practices and regulations — for example, HIPAA in healthcare, PCI in retail and Sarbanes Oxley (SOX) for public companies — as well as expertise with the specific technology architecture in use in your enterprise.



Consultative approach to 'operationalizing' security

When it comes to security, one size definitely does not fit all. Look for a security provider that will help you create a security program customized to meet the specific needs of your company — not a blanket program that is rolled out to all customers. This type of provider will make it their business to understand your business. This is key to 'operationalizing' security within your organization — the building in and ingraining of a security policy and security awareness throughout your organization, your employees and processes — the crucial process that takes into account your people, processes, technology, and policy to create a lasting, sustainable security program that minimizes your risk and impact. Their processes should include upfront planning sessions to get a good understanding of your business, including your day-to-day processes as well as your technical and business concerns and goals. Armed with jointly developed plans and criteria, a vendor can properly weight the importance of network assets and known network issues to create a security plan that is properly prioritized.

Reputation, reputation, reputation

Conduct research as required to make sure the company is qualified and highly reputable. Questions to ask include:

- How many employees are in the company?
- What types of background checks are performed on employees?
- What types of security certifications are employees required to hold?
- Who will have access to your information? Do all those workers have the right credentials and background checks?
- How long has the company been in business?
- How long does the average employee remain with the company? What is the average number of years of service of current employees?
- Does the company have experience with the networks equivalent in scope, size, and technologies to your network?
- Can the company provide sample reports and documentation of processes?

- What internal processes are in place at the MSSP to prevent their employees from abusing access to your network?

Employee qualifications

Ask about the caliber of the employees. Look for firms who hire only experienced and very seasoned professionals. Inexperienced workers may primarily search for red flags in the system, but will lack the real world expertise required to fully understand what that particular flag means to your company. Questions to ask include:

- What is your hiring process?
- What level of experience is required for employees, and where have they obtained that experience?
- How are employees tested to ensure that their level of expertise meets company requirements?
- What ongoing training/education is available to keep employee skills current, aware of the most recent threats and how to mitigate those threats?
- What is the typical profile of the type of employee that would be working on my account?

Proven around-the-clock coverage

- Many vendors will claim to offer 24x7x365 monitoring. Be sure to ask about the infrastructure that supports this offering. For example:
 - Do the security operations centers (SOCs) have the global reach and scalability required to meet your business needs?
 - Are facilities staffed appropriately, with the same level of staff expertise and capabilities around the clock?
 - What happens if a natural disaster or power outage strikes — what contingency plans and documented processes are in place to assure seamless and continual monitoring?

Responsiveness

The vendor you select should offer the rapid response times required to minimize risk and provide maximum protection for enterprise and customer data. The vendor should be able to demonstrate proven response times and practices that enable rapid identification and containment of incidents.

Converged solution expertise

Your security vendor needs to demonstrate expertise across the products and services you have in place today, as well as those planned for tomorrow, including wireless LANs as well as wired LANs, public wireless carriers, Voice-over-IP, integrated voice and data devices and more.

Proficiency in monitoring networks of your size

Large networks generate large amounts of security data every minute of the day. Ask about procedures in place to collect, analyze and report on network activity. Make sure the vendor you select demonstrates the ability to:

- Collect, correlate, analyze and interpret large volumes of information from many data sources to ferret out meaningful events, and
- Report events to you in terms of the impact on your network, the specific assets that are impacted, and what it means to your business.

True data interpretation

Assessment. Any vendor can run a scan tool and provide you with the reports from that tool. You need a vendor that can take the wealth of information provided by standard tools and provide a rich interpretation of the data. For security assessment activities, you should receive a detailed description of the gaps and weaknesses in your network, mapped to your business assets so you can truly understand and assess the impact that those gaps and weaknesses can have on your business. In addition, an action plan to address those weaknesses should also be provided, prioritized by potential impact those weaknesses can have on your business — rather than just a list of weaknesses.

Day-to-day monitoring. For network monitoring activities, look for vendors that can rapidly detect and characterize anomalous, suspicious or malicious activity, and not only report the incident, but also provide a complete plan to minimize exposure and contain the incident as quickly as possible — instead of a vendor who will simply alert you to security incidents that were flagged by your security devices.

Ability to provide interactive support

The level of support you require will depend upon the level of expertise you have in-house. In the event

you choose to outsource most of your security requirements, your in-house expertise may be limited. Your vendor should offer a highly interactive service approach, and be able and willing to walk your workers through the actionable remediation steps required to contain a breach.

How to best partner with your security vendor

Once vendor selection is complete, and corporate agreements are signed, including a non-disclosure agreement (NDA) and SLA, there are steps you can take to provide a strong working relationship with your MSSP — a relationship that will help you get the most value out of your managed services:

- Know and be able to articulate your high-level strategic business goals as well as technical network concerns. This will allow your vendor to create rich security plans that also address strategic business objectives.
- Know and be able to express what aspects of security are most critical to your business — for example, PCI or HIPAA compliance, or preservation of intellectual property. This will help your vendor properly prioritize security initiatives.
- Know and be ready to share network topology diagrams and all policies (regional, corporate, firewall, router configurations).
- Provide your vendor with a single point of contact, providing a clear line of communication between the businesses.
- Be able to provide all previous reports, assessments and information on past security breaches
- Provide your near- and long-term planned network changes

Summary

Should you use in-house resources or outsource network security assessments and day-to-day network monitoring? At the end of the day, it's all about how you can best mitigate risk. The corporate team should always retain ownership of your security plan strategy — that initiative is too crucial to turn over to a vendor for outsourcing.

The added value of a strong MSSP relationship

When your MSSP is also a trusted advisor, sharing high-level business concerns and goals can result in rich security plans that also address key business objectives:

The enterprise issue:

A very large manufacturer and distributor retained an MSSP to assess the security of their network. During the initial meeting, the company shared their concerns about the inability to secure wireless networks and devices — and the resulting company moratorium on wireless solutions — as well as their need to improve productivity throughout the company.

MSSP assessment results:

An examination of the network revealed that employees who needed wireless technologies were simply filling the void themselves using rogue wireless devices — creating a substantial yet undiscovered network weakness. A closer look at which employees were using wireless and why revealed how the deployment of mobility solutions in the sales force, warehouse and production line could help the company meet target productivity improvements — a key high level strategic business goal.

The solution:

After demonstrating that today's security protocols and monitoring technology could provide a level of security equal to that of wired networks, the MSSP recommended the deployment of a secure wireless solution that:

- Resolved the tactical network weakness associated with the presence of rogue wireless devices, and
- Achieved a core strategic objective by enabling the company to meet target goals for productivity improvements

Yet it makes great sense to seek outside assistance for many of the day-to-day tactical and operational elements of the plan strategy, and to gain the perspective of outside experts to help construct an appropriate plan. In addition, once your security plan is created, there is also considerable value in obtaining an independent external view of your plan, the threat landscape and the technology and tools that could impact that plan.

The statistics point to managed security service providers as the better choice. The Verizon 2008 Data Breach Investigations Report, which compiles the forensic analysis of 500 security breaches, reveals a number of statistics that substantiate this statement:

- 75 percent of the breaches were discovered by a third party
- 87 percent were considered avoidable if basic security controls had been in place at the time of the attack
- 62 percent were attributed to a significant error
- 22 percent of the attacks exploited a known vulnerability — and 90 percent of those attacks had patches available for at least six months prior to the breach that could have prevented the breach

States the report: "The fact of the matter is that though most organizations have the technologies, people, and know-how required to detect and respond to data compromise events, they seldom do so. In 82 percent of cases, our investigators noted that the victim possessed the ability to discover the breach had they had they been more diligent in monitoring and analyzing event-related information available to them at the time of the incident. The breakdown is in the process. What these organizations seem to lack is a fully proceduralized regimen for collecting, analyzing, and reporting on anomalous log activity."⁶

Industry analyst Gartner confirms the benefits companies can expect from outsourcing security:

- Improved service levels and skill sets
- Reduced costs
- Better focus on core business
- Improved ROI from IT
- Shorter implementation times⁷

And as a result of the reduction in risk and the strong benefits, analyst firm The Yankee Group predicts that 90 percent of big U.S. companies will outsource security to MSSPs by the end of the decade.⁸

For more information on network security, please visit www.motorola.com/business/services.

About Motorola's Managed Security Services

Securing networks is more than just applying security controls and devices to a network. Motorola's Managed Security Services begins with understanding your environment, including the network, applications, and services, end to end, and its users. Our approach to security encompasses people, processes, policy, and technology, bringing security to your entire operational environment and helping to institutionalize security — the key to a successful security program.

Motorola Security Assessment

Motorola's Security Services address the complicated security challenges of today, helping you prepare and plan for real-world security threats and achieve the level of network security necessary to accomplish your business mission and objectives. It begins with a comprehensive assessment that examines key aspects of your network infrastructure and security program, including existing technologies, operational security, incident response procedures and physical security. The assessment identifies and evaluates vulnerabilities and risk, then provides actionable recommendations for mitigating the risks and protecting vital enterprise assets and infrastructure. This allows you to understand and manage risk, define budgets, and achieve secure and reliable communications.

The Security Assessment Services include field-tested techniques and procedures for assessing security vulnerabilities in all elements of your communications network, whether wired, wireless or two-way radio. Motorola offers security professionals with the highest qualifications — in addition to multiple security credentials, our professionals are all specially trained and credentialed in the protection of mission critical enterprise network infrastructures.

Motorola IT Security Monitoring

For enterprises, the availability, confidentiality, and integrity of the network are crucial. The ability to predict, rapidly detect, characterize, and respond to security incidents is key to minimizing the impact of security events. Motorola's Security Monitoring service provides the peace of mind that only comprehensive and proactive 24x7x365 security monitoring services can provide. Combining expert visualization and correlation capabilities with around-the-clock vigilance, Motorola IT Security monitoring detects potential threats and minimizes your exposure to localized or system-wide security breaches. Real-time data, prompt response, and expert security remediation assistance allow you to exercise greater control and ensure reliability. The service also aids in appropriate response and recovery efforts designed to maintain the integrity and availability of network resources and information.

In addition to providing these services to many large and complex mission critical and service provider grade networks, we utilize our own services to secure our own networks — using the same Security Operations Center (SOC), the same people and the same tools. A Fortune 100 multi-national company, Motorola's own security monitoring services protects our expansive network every second of every day — a network that encompasses all 320 of our facilities in 73 countries, serving over 60,000 employees.

With access to leading security experts, strong ties to the global security community and the resources of Motorola's 75-year history of communications security, Motorola Security Services help you safeguard business-critical IT systems and better protect the employees and customers who depend on their operation.

To find out how you can put our security expertise to work in your enterprise, please visit www.motorola.com/business/services or contact your Motorola Enterprise Mobility representative.

For more information

For additional information on security, please visit the Motorola website to download the following white papers:

- The Need for Wireless Intrusion Prevention in Retail Networks
- What Every Retail CIO Needs to Know about PCI Compliance and Secure Seamless Mobility



Citations:

1. Information security breaches quadrupled in 2007; The Register; January 2, 2008; John Leyden
2. How much do security breaches cost anyway?; The Register; April 12, 2007; John Leyden
3. Three of Four Say They Will Stop Shopping at Stores that Suffer Data Breaches; Information Week; Sharon Gaudin; April 12, 2007
4. Supermarket loses 4.2 million credit card details; The Register, John Leyden; March 18, 2008
5. Why Enterprises Outsource Network Security; Michael Suby; Stratecast Partners, a division of Frost and Sullivan, November 2005
6. 2008 Data Breach Investigations Report; Verizon Business Risk Team
7. Benefits of outsourcing, according to Gartner (Security Outsourcing Grabs Hold, Bill Brenner; CIO Decisions Magazine
8. Report says Virtually All Big Companies Will Outsource Security by 2010; Gregg Keizer, TechWeb News, InformationWeek, August 23, 2004



MOTOROLA

motorola.com

Part number WP-VC6096. Printed in USA 10/08. MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners. ©2008 Motorola, Inc. All rights reserved. For system, product or services availability and specific information within your country, please contact your local Motorola office or Business Partner. Specifications are subject to change without notice.