

THE POWER TO *stop*
INTERNET THREATS BEFORE THEY

impact YOUR BUSINESS.



***How to Select a
Managed Security Services Provider***
A Comprehensive Guide and Checklist for Enterprises

 INTERNET | SECURITY | SYSTEMS®

Ahead of the threat.

Contents

HOW TO SELECT A
*Managed Security Services
Provider*

- I Introduction
- II Why Choose to Outsource?
- III Selecting a Managed Security Services Partner
- IV Conclusion
- V About Internet Security Systems
- VI Managed Security Services Provider Checklist

I. Introduction:

Enterprises today are locked into a continuing battle with online enemies that are smart, destructive and can strike at any moment. Given the wide variety of online threats that businesses face — from viruses to denial of service attacks and unauthorized Web site access — it comes as no surprise that companies managing their own information security often fall short of the in-house resources needed to protect online systems on a 24/7 basis.

During an attack, technology cannot operate unattended. Sophisticated security requires highly skilled personnel who can be expensive to recruit, hire and retain — a challenging problem for firms with limited IT budgets. Without expertise and resources to appropriately manage, monitor and protect your security posture on a 24/7 basis, the effects could be devastating to your infrastructure. In addition, organizations need protection that can be guaranteed without sacrificing service quality, business continuity and return on investment.

The reason why the market for managed security service providers (MSSPs) is growing at such a rapid pace: the need to act instead of react. This executive brief was created to help advise you on the benefits of choosing to outsource, as well as how to select an MSSP that will best suit the needs of your organization.

II. Why Choose to Outsource?

By outsourcing security operations to an MSSP and taking advantage of its expert tools, skills and processes, enterprises can improve system uptime and performance while avoiding making a large investment in technology and resources.

Not only do MSSPs help protect companies that do not have the manpower or budget to build and operate security infrastructure on a 24/7 basis, but they can also increase productivity. Allowing an MSSP to handle day-to-day security monitoring and management gives organizations an opportunity to allocate in-house IT resources to more strategic initiatives.

MSSPs also facilitate business continuity by providing advanced intelligence to thwart attacks before they cause damage and disrupt business operations. This layer of proactive protection lends a competitive edge by ensuring that businesses will remain functional — even when a sophisticated new virus or worm is spreading rapidly across the Internet.

These potential benefits of outsourced security can only be achieved by selecting the right managed security services provider. This brief is designed to assist you in the evaluation process to ensure the potential provider you select will best protect and service your vital IT assets.

According to the 2003 CSI/FBI Computer Crime Survey, one in two organizations suffer from a serious security breach every year, involving theft of proprietary information, sabotage of data and financial loss. Of those organizations suffering a security breach, 99 percent had both firewalls and antivirus in place.

The British security firm mi2g estimates that in February 2004 alone, hacker attacks caused between \$68 billion and \$83 billion in damages worldwide.

III. Selecting a Managed Security Services Partner

According to the Infonetics Research *World User Plans for Security Products and Services* study, the following are the top five key vendor provider selection criteria for organizations choosing managed security services:

1. Security expertise and reputation
2. Compatibility with existing equipment
3. Service and support
4. Financial stability
5. Broad range of VPN and security services

When evaluating potential managed security service providers to become your company network's eyes and ears, the selection criteria become imperative. ISS has developed a set of guidelines and questions to help you evaluate potential MSSPs.

IIIa. Security Expertise and Reputation

Page 3

Among the key elements that come into play when it comes to the expertise and reputation of an MSSP are the skills and longevity of the staff in its security operations center, customer satisfaction and the managed security service provider's (MSSP) history and investment in security research. The reputation and experience of the service provider in your company's industry is a critical factor in your decision, as they will understand your specific needs and pains.

IIIb. Compatibility with Existing Equipment

Page 3

In addition to managing and monitoring your security posture on a 24/7 basis, your MSSP must have the capability and necessary certification to protect your current equipment.

IIIc. Service and Support

Page 4

Any service provider can claim they respond rapidly and thoroughly. The provider you choose should offer more than just a rapid response guarantee, but also a guarantee of protection against emerging Internet threats. The provider must be willing to stand behind these commitments in a legal document known as a service level agreement (SLA).

IIId. Financial Stability

Page 6

One of the most important criteria to consider when evaluating managed security service providers is their financial stability. Managing security on an outsourced basis for large numbers of customers requires significant capital and resource outlays to develop new technologies, operate a global network of security operations centers, and attract and retain knowledgeable and motivated personnel. As with any other business decision, look for selecting a managed security services partner that is financially stable, with deep resources and a sustainable business model.

IIIe. Offers a Broad Range of VPN and Security Services

Page 6

Your security needs are continually evolving with the influx of new worms and viruses and changing regulatory requirements. Ensure that any managed security services partner offers a comprehensive suite of vulnerability assessment and management services that will protect you ahead of threats.

IIIa. Security Expertise and Reputation

What customers do you currently manage in my industry?

- Check the provider's knowledge and understanding of common pains and needs of companies in your industry.
- Do their customers have similar needs to yours in terms of network size, threat exposure, regulatory compliance requirements, etc.?

Are you able to provide references and case studies for customers in my industry?

- Contacting references for feedback is critical before selecting a managed security services partner to whom you can feel comfortable entrusting your network security.
- Case studies are helpful to determine whether the MSSP has a solid grasp of the needs of companies like yours. Case studies can also provide you with new ideas and methods that the MSSP can use to help increase your company's internal efficiencies and operations.

How long have your oldest customers been with you?

- Look for a provider who has successfully retained customers for several years, showing strong customer satisfaction.
- Ask what their average customer churn rate is — look for key, long-term (3+ years) customers in industry and/or with network needs similar to yours.
- Ask to see results from current customer satisfaction research conducted either internally or by a third-party vendor.

IIIb. Compatibility with Existing Equipment

Are you able to manage other technologies I may have in place or am planning to implement?

- Ensure that the MSSP is able to manage whatever equipment you are currently using to avoid unnecessary changes and costs to implement new technologies.
- Look for MSSPs that have extensive experience in managing several technologies and platforms, in addition to their own suite of products.
- Ask for a list of platforms that the MSSPs hold certifications with a given technology to manage. If your current platform does not appear on the list, ensure that you check with the provider to see if they can customize their services to suit.
- Look into whatever product technology the MSSP offers to see if it fits your company's needs.

What is the “word on the street” about your company?

- Ask for recent analyst reports in which the MSSP has been mentioned or compared with competitors. Ensure that you receive a non-biased explanation of the results.

How much focus do you place on security intelligence?

- The MSSP you choose should have extensive, top-tier internal and external resources to continually stay on top of the latest attack strategies, network threats and vulnerabilities. Strong research and development teams, special operations groups and global vulnerability/threat analysis processes are crucial to keep companies protected from the constantly-evolving attack schemes and technologies.
- A heavy focus on discovering and researching security vulnerabilities (while working with the affected vendors to get them fixed) means that your systems will be updated and protected before having the chance to be impacted.

IIIc. Service and Support

What are your policies and average adherence rate for Service Level Agreements (SLAs)?

- Any service provider can claim they respond rapidly and thoroughly. The MSSP should have well-defined service level agreements, including processes and time periods within which the company will respond to any security need. The agreements should include specific steps to be taken in the event of a security incident, as well as procedures the company takes to assure that the same system intrusions do not happen again.
- Look for an MSSP that takes accountability for managing your network by offering more than just a rapid response guarantee, but also a guarantee of protection against emerging Internet threats. The provider should also allow you to recoup a portion of losses in the event the service does not deliver as promised.
- Keep in mind that a credible service provider should offer comprehensive, detailed and guaranteed SLAs for all of its offerings. Make sure the SLAs include commitments for initial device deployment, incident response and protection, requests for security policy and configuration changes, and for acknowledgement of requests.
- Ask the providers for their average SLA adherence rate.

What are the hours of your security operations center and are you sufficiently staffed to manage my network?

- Security incidents happen at all hours, not just between 9 a.m. and 5 p.m. You need to evaluate whether your managed security services partner is sufficiently staffed on a 24/7/365 basis to ensure adequate protection for your company. Properly staffing a security operations center seat around-the-clock requires six full-time security management analysts. This is required to cover all hours in the day including vacation, sick leave, training, etc.
- Ask the provider how they staff each seat in their security operations center — are they sacrificing late night coverage or engineer training to reduce their staffing expenses? Anything fewer than six engineers per seat could leave your network at risk.

How have you handled security incidents in the past and do you have well-defined policies, procedures and time periods for response to security issues?

- Ask for specific examples of how the company has handled security threats.
- Check to see that they have a proven history of successfully handling and communicating threats with each customer and ask to see samples of specific processes and time periods for response to security issues.
- Ensure the provider has detailed, well-tested emergency response capabilities, well-defined, specific processes in the event of a security incident and detailed measures established to ensure that system intrusions do not repeat.

Do you provide secure, real-time, online access to the status of my network, service data and metrics as well as capability to generate reports?

- The speed at which security trends emerge dictates that access to security information and intelligence must be immediate and always available. MSSPs must provide customers with a comprehensive online resource that provides detailed information about services being delivered, and how your security posture relates to overall industry trends. The best Web portals will cater to multiple levels within your organization and offer reporting that is appropriate for not just the front line security analyst, but management and executives alike.
- Ensuring that your provider's Web portal is feature-rich means that you should never be kept in the dark when the security operations center is supporting an issue on your behalf. Be wary of providers who "keep the curtains closed" and hide the details of trouble ticket work logs and notes. Always be sure to ask what information is stored in the ticket that is not visible through the online interface. Generally speaking, your provider should operate in a manner similar to an in-house security group, and the provider should be forthcoming with information and necessary details.

Continued next page.

- Specific features to look for in an online portal include:
 - ♦ An Internet threat index that provides a quantitative measurement of potential risk as well as a verbose assessment
 - ♦ Real-time and historical log analysis engine
 - ♦ Tools that enable the tracking of worm propagation throughout the enterprise
 - ♦ Overview of services provided with customizable views
 - ♦ Online helpdesk with interactive trouble ticketing and submission
 - ♦ A detailed reporting package that covers the breadth of all services and is suitable to a variety of different audiences
 - ♦ Real-time reports that show the provider's compliance to contractually agreed-upon Service Level Agreements
 - ♦ Detailed security intelligence that makes the portal your number one site to visit each day

Do you have best practice-based policies and procedures for your own systems and security operations centers in case of emergency?

- Security operations centers are strategically located, technically advanced facilities designed to remotely manage, support and respond to threats and vulnerabilities 24/7. In addition to asking the MSSP about its security operations centers' capacity to staff security engineers, it is also important to inquire about the capabilities and operational standards of the facility. A provider should have multiple, fully operational centers that are ready and able to accept each other's loads in the event that any particular threat or disaster disables a center. Outsourcing security to a provider with only one security operations center will unduly expose your network to unnecessary risk — if that single operations center loses Internet connectivity, your network will be left unprotected.
- Obviously, the security operations centers should be monitored 24/7/365 — not only by the security specialists that monitor each customer's systems, but also by personnel dedicated to infrastructure support. This way, customers never suffer the results of a problem within the security provider's facilities. Pay attention to how the provider manages network connectivity, bandwidth, carrier relations and device health. If the provider cannot show best practice-based policies and procedures for its own systems, you cannot be certain that those systems will be able to serve your company.
- Make sure that the provider's own infrastructure is well-protected. Consider the location of the company's security operations centers. A managed security service provider should

locate its facilities in a low-risk threat zone and house its operations within a disaster-resistant or hardened facility, built according to the area's risk profile. The security operations centers must be built and maintained to strict standards to ensure that operations continue seamlessly, regardless of natural disaster, total loss of power or physical break-in. It should meet a variety of key standards including National Fire Protection Association (NFPA) 1600, ISO/IEC 17799 and Federal Financial Institutions Examination Council (FFIEC) compliance and Statement of Accounting Standards (SAS) 70 among others. Compliance with these key standards should be a basic metric by which you judge a managed security service provider's preparedness and effectiveness

Do you have a global presence?

- An international presence is critical for any enterprise that conducts business in a global economy. You will want to work with a company that has security operations centers and security research sites all around the world. Cyber-criminals can work from anywhere. Indeed, many of today's most dangerous viruses and other attack mechanisms are created in developing countries where attention to such acts may be weak or nonexistent. A company with security operations centers and research facilities near the source of such activity will be able to identify and protect customers worldwide from dangerous attacks.


IIId. Financial Stability

What is your financial picture and growth model for Managed Security Services?

- Ensure that the provider you select has the financial resources to continually invest in improving their service offerings and capabilities. Examine the company's business model. Look at the provider from the standpoint of its own investors. When evaluating a potential provider look at their overall financial standing, and that of the MSSP business itself. When possible choose a provider whose managed security services business is prosperous and not dependent on other lines of business to remain afloat. If their model is sustainable, it is less likely you'll find yourself the victim of obsolete technology or a provider who goes out of business.
- If the MSSP is privately held, inquiries about its funding may provide insight into the stability of the organization. Are plans for further development or future service offerings contingent upon an upcoming round of funding? With venture capital becoming increasingly difficult to obtain, you do not want your provider's service contingent upon its ability to close a new round of funding.
- A provider must extend significant resources toward attracting the most experienced, qualified network security professionals, and toward the development of sophisticated protection strategies for the benefit of their clients.

IIIe. Offers a Broad Range of VPN and Security Services

What other security services and technology do you offer?

- Evolving security needs require a great breadth of services — including elements that you may not need now, but that might become compelling as your company grows. Make sure you select a provider with a full suite of services to offer you as your requirements change.
 - Look at the company's record of innovation and plans for future service offerings. You will want to partner with an information security provider that grows and innovates along with your systems and the overall information security landscape.
- 

IV. Conclusion: Secure Your Online Assets with a Proven Service Provider

Outsourcing security enables organizations to improve their security position, lower their overall cost of doing business, and focus key IT personnel on core business functions. Central to the success of a security outsourcing decision is the choice of provider. Look for a provider who has a history of leading-edge service and financial stability, bulletproof service level agreements with

guaranteed protection, a redundant global network of security operations centers staffed by experienced security experts and a comprehensive, continually evolving set of services. With a broader perspective on key evaluation criteria, you can now ask the right questions to identify the best provider of managed security services for your business.

About Internet Security Systems (ISS)

Internet Security Systems has long been a trusted security expert for world governments and the Global 500. For these elite clients, and now for small and mid-size organizations, ISS provides preemptive security products and services that stop Internet threats before impact. Founded in 1994, ISS is publicly traded on the NASDAQ (ISSX) and headquartered in Atlanta. ISS protects more than 11,000 global customers, and maintains 1,200 employees operating in 27 countries.

To learn more about ISS and guaranteed protection, visit www.iss.net, call 800-776-2362, e-mail at sales@iss.net or find an office location near you <http://www.iss.net/about/locations/>



V. Managed Security Services Provider Checklist

1. Security Expertise and Reputation

- Key, long-term (3+ years) customers in industry and/or with network needs similar to yours.
- Proven history of handling threats with each customer.
- References and case studies available for customers in your industry.
- Strong international presence: security operations centers and security research sites all over the world.
- Extensive top-tier internal and external resources (including strong research and development teams, special operations groups and global vulnerability/threat analysis processes) directed at the latest attack strategies, threats and vulnerabilities.

2. Compatibility with Existing Equipment

- Flexibility and capability to manage your existing platforms.

3. Service and Support

Service Level Agreement Terms:

- Service agreements that provide guaranteed levels of protection with a money-back warranty.
- Clearly defined processes for validation of service level changes.
- Clearly defined, rapid time periods with which validated changes will be implemented.
- Offers guaranteed, money-back warranty.

Staffing Policies:

- Proven ability to provide full-time security services, 24/7/365.
- Six engineers per seat in the security operations center.
- Clear data and methodology for predicting security operations center activity on a per-seat basis.
- Clear identification of personnel for your account.
- At all times of the day, Level I analysts should not be without higher-level backup/support.

Processes and Procedures:

- Specific processes and time periods for response to security issues.
- Well-defined, specific processes in the event of a security incident.
- Well-defined measures established to ensure that system intrusions do not repeat.
- Best-practice based policies and procedures for its own systems.
- Compliance with key industry standards: NFPA 1600, BS7799, FFIEC and SAS-70.

3. Service and Support *(continued)*

Online Access to Service Data and Metrics:

- A secure Web-based tool for intelligence and reporting.
- Internet threat index and assessment.
- Real-time and historical log access.
- A variety of reporting options covering the breadth of all services and suitable for multiple audiences.
- Online helpdesk with interactive trouble ticketing.

Security Operations Center Capabilities and Standards:

- State-of-the-art technology.
- Multiple, fully operational, fully redundant security operations centers located worldwide.
- Infrastructure support and customer support.
- Infrastructure located in low-risk threat zones, housed within disaster-resistant/hardened facilities, built according to the area's risk profile.
- Operations well-distributed, designed to back each other up.

4. Financial Stability

- Deep financial resources and stability to continually invest in service improvements.
- Stable, profitable, sustainable business model; likely to remain current and thrive over time.
- Not dependent on upcoming rounds of venture capital/investment funding.
- Significant size to handle multiple customers and attacks simultaneously.
- Sized sufficiently to scale with growing customers.

5. Offers a Broad Range of Security Services

- Record of innovation that supports growth and evolution of customer security needs.
- Full range of services that extends far beyond current needs.

GLOBAL HEADQUARTERS

6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236-2600
e-mail: sales@iss.net

REGIONAL HEADQUARTERS

Australia and New Zealand

Internet Security Systems Pty Ltd.
Level 6, 15 Astor Terrace
Spring Hill Queensland 4000
Australia
Phone: +61 (0)7 3838 1555
Fax: +61 (0)7 3832 4756
e-mail: aus-info@iss.net

Asia Pacific

Internet Security Systems K. K.
JR Tokyu Meguro Bldg. 3-1-1
Kami-Osaki, Shinagawa-ku
Tokyo 141-0021
Japan
Phone: +81 (3) 5740-4050
Fax: +81 (3) 5487-0711
e-mail: sales@isskk.co.jp

Europe, Middle East and Africa

Ringlaan 39 bus 5
1853 Strombeek-Bever
Belgium
Phone: +32 (2) 479 67 97
Fax: +32 (2) 479 75 18
e-mail: isseur@iss.net

Latin America

6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236-2709
Fax: (404) 236-2629
e-mail: isslatam@iss.net

Copyright© 2004 Internet Security Systems, Inc. All rights reserved worldwide.

Internet Security Systems, Proventia and SiteProtector are trademarks, and the Internet Security Systems logo and X-Force registered trademarks, of Internet Security Systems, Inc. Other marks and trade names mentioned are the property of their owners, as indicated. All marks are the property of their respective owner and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.

MC-EXCBRF-604

 **INTERNET | SECURITY | SYSTEMS®**

Ahead of the threat.