

Managed Security Services for SMBs- A Key Consideration

For many large organizations, security has certainly moved from the backroom to the boardroom. Increased focus on compliance regulations has also seen C-level executives playing an increasingly active role in formalizing corporate security policies, be it data security or otherwise. Indeed, the recent creation of the roles of CSO (Chief Security Officer) or CISO (Chief Information Security Officer) appears to validate this assertion.

It was recently reported by Symantec¹ that between July 1 and December 31, 2005, there was an average of 39 attacks *per day*. These include all malicious attempts to access a network, including attacks blocked at the firewall and network intrusion detection system levels. In addition, Symantec reported the average number of denial of service (DoS)² attacks detected per day was 1,402, an increase of 51% from the first half of 2005.

Supporters of network security have highlighted different scenarios where dire consequences of security breaches may include:

- **Loss of productivity.** When employees are unable to access critical information located on the network.
- **Loss of revenue.** When customers or suppliers are unable to access the website, process or place orders. The actual costs of downtime vary according to length of downtime, company size, industry and reliance upon the network and/or Internet. Some studies have indicated that the cost of network downtime may run up to hundreds of thousands of dollars on an annual basis. For instance, for a trading company with 10 employees having a turnover of S\$1.6 million per annum, an hour of downtime can cost over S\$800. Assuming that a network experiences 4 hours downtime due to security breach, this would cost the business S\$3200 per incident!
- **Loss of confidence and increase in customer dissatisfaction.** Especially when confidential client information has been misappropriated, the impact of such “soft” indicators is harder to quantify but no less important to a company’s goodwill and/or brand equity. This is especially acute for online businesses without a physical shop front where the reputation of the organization is crucial for its survival.

¹ Symantec Internet Security Threat Report Volume IX: March 2006

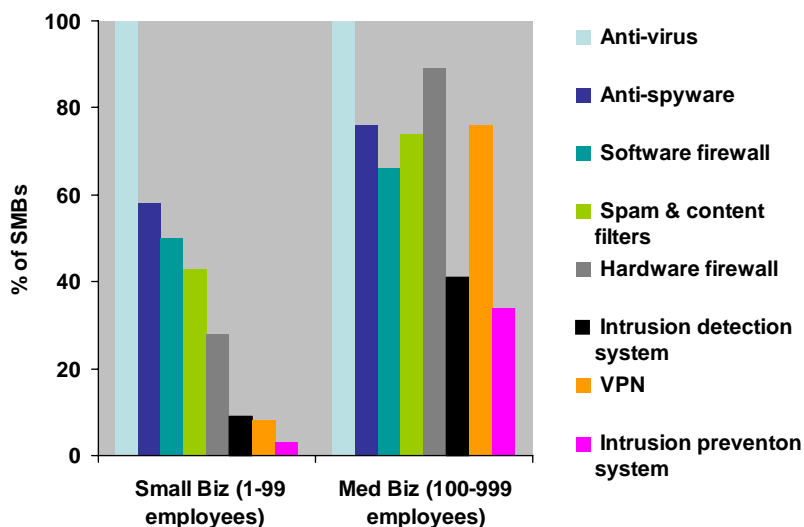
² A denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users and usually targets web servers, causing the hosted web pages to be unavailable on the Internet.

The importance of security has also been acknowledged by decision makers in smaller companies. In most cases, the responsibilities for IT security would be held by systems administrators or senior IT managers for medium-sized businesses, or with the business owner for micro businesses with less than 5 employees. In fact, a recent survey of over 300 SMBs in Singapore revealed that 40 per cent of small businesses in Singapore with 1-99 employees, do not have anyone providing IT support, be it insourced or outsourced.

Due to the lack of available skills and resources, many small businesses adopt a fairly reactive stance towards security, hoping that nothing untoward would happen to their networks or data. Investments in security, then, are often regarded as a necessary evil. The same study found that 18 per cent of companies having less than 20 employees had formal security policies in place, compared to 90 per cent of medium-sized companies with 500-999 employees.

In terms of security applications being used, it was found that the ubiquitous anti-virus application has reached saturation amongst PC-enabled SMBs with 1-999 employees (see diagram below). To a large extent, this is because many PCs and notebooks are now sold with pre-loaded security applications.

Figure 1. Type of security applications used by Singapore SMBs



Source: PacNet IP Index, June 2006

The exponential growth in the variety of malware has witnessed a proliferation of security applications, designed to protect the network or PC in different ways. This has often resulted in companies using different brands of security applications within one system, each with different discreet functions such as anti-virus, anti-spam and anti-spyware.

Security vendors have been quick to recognize that SMBs have an acute need to streamline their security applications. To this end, some leading security vendors have been quick to develop integrated “everything but the kitchen sink” type of security applications tailored for small and medium-sized organizations, such that only one brand of security solution is used. Even still, managing security applications is sometimes a painful process for the busy IT person and even more so for the small business without an IT resource.

Managed Security Services: A viable option for SMBs

The other option that SMBs have not fully investigated is managed security services. A managed security service provider (MSSP) is an Internet service provider (ISP) that provides services such as virus blocking, spam and content filtering, intrusion detection, firewalls, and virtual private network management. In most cases, a MSSP can take responsibility for system changes, modifications, and upgrades. The adoption of managed security services is an optimal choice for businesses that lack internal IT resources and/or those that want to attempt a piece-meal approach to security outsourcing.

To date, we have found that over 65 per cent of MBs and over 75 per cent of SBs are insourcing security respectively. The key reason given for not outsourcing IT security is the commonly held belief that the user organization has the requisite in-house capability to manage security. Other reasons include the perception that security outsourcing is expensive, together with a lack of trust of managed security providers.

Benefits of Managed Security Services

Despite this, the benefits of managed security services cannot be ignored. These include:

- Reduction in overhead costs or other CAPEX and freeing up of scarce IT resources and non-IT resources (for the case of the micro business) to focus on core business activities;
- Reducing risk by placing control of a key operation in the hands of more highly-skilled professionals and thereby partially transferring responsibility;
- Access to industry best practices for proactive threat prevention at fairly reasonable price points, and



- Reduction in downtime and improved performance through robust monitoring of the network on a 24X7X365 basis.

The concept of security outsourcing may often appear daunting to many SMBs. To this end, many organizations start by partially outsourcing small chunks of network security such as:

- Network firewall monitoring
- Managed anti-virus
- Encryption/ Authentication
- Content filtering
- Intrusion detection/ Intrusion Prevention

Amongst the aforementioned, the most commonly outsourced area by SMBs in Singapore is antivirus protection. Nowadays, this is commonly offered by MSSPs as a bundled solution with anti-spam capabilities in a managed email security solution.

Managed Email Security Services

Essentially, this service ensures that all incoming messages are centrally scanned before entering the company's network gateway so that:

- The company's valuable bandwidth and mail storage is not taken up or "wasted" on spam emails while employee productivity is optimized, and
- Virus threats which are most commonly passed via infected emails are alleviated, thus reduce the incidences of server or PC downtime.

All incoming emails are filtered against regularly updated databases of known viruses. Intelligent algorithms are applied to check for spam email, such that only "legitimate" email is received by the mailbox owner while suspect email is routed to a virtual quarantine or holding area to be examined by the recipient at his or her convenience. Managed email security services are usually also available for employees who work remotely.

Because the service provider is likely to handle a large amount of e-mail traffic from different clients, new security threats can be analyzed and identified before they are officially published, acting as a critical first line of defense.

Inhouse administrators or users of managed email security solutions should usually have access to an intuitive interface that allows for real-time configuration, customization of filters and policy management specific to each company's needs and requirements.

Managed Firewalls Services

Where network protection is concerned, SMBs can also consider managed firewall services. Many small SMBs find cash flow management a real challenge, with investments in IT infrastructure often perceived burdensome. In a managed firewall situation, the vendor provides the necessary hardware firewall on a loan basis, so that the user organization need only pay for the security service on an affordable monthly basis.

The benefits of having a managed firewall service are pretty similar to that of a managed email security service, in that:

- The user organization is free to focus on its core business while safe in the knowledge that it would receive the most updated protection from the service provider, including 24x7 technical support, management and maintenance;
- The user organization has the flexibility to upgrade or expand the service as and when the business grows; and
- The user organization will be able to receive preventative monthly monitoring reports of network traffic and intrusions.

Nowadays, managed firewall solutions also come with the option of integrated managed virus protection so that the user organization need only consult one service provider for all managed security needs.

Choosing the Right MSSP

When queried about the selection criterion for managed security providers, SMBs were quick to list the following as primary considerations:

- **Price.** The ROI of managed security services is often hard to quantify, especially when it involves measuring the opportunity cost of employee time. However, for small businesses with scarce IT resources, this becomes a very compelling value proposition. In any case, the price points associated with a managed security service should be affordable with flexible payment options.



- **Level of competence.** The MSSP should be evaluated on its competency in IT security, level of certification of staff, accreditation and track record. References should be sought to establish vendor credibility.
- **Good reputation and longevity.** Decision makers should evaluate the business health of the service provider's to avoid partnering with a provider that may not be around in the next 24 months.
- **Service Level Agreements.** Companies need to ensure that service level agreements (SLAs) are established and that the service provider can be made liable for any lapses in service levels. In addition, SMBs considering managed security providers should also take into consideration the ease of use of the service and access to regular reporting.
- **Scalability.** Decision makers should ensure that their solution is scalable so that that can upgrade or add solutions as the company grows.

With such considerations in place, SMBs will definitely be able to harness the benefits of managed security services, enjoying the peace of mind that comes from knowing their systems are protected by experts and leveraging the opportunity to better concentrate on their core business.

About AMI-Partners

Established in 1996, AMI Partners is headquartered in New York City, with a network of offices and affiliates in Houston, San Jose, the U.K. (London), Japan (Tokyo), India (Kolkata) and Singapore. AMI specializes in ICT solutions & Business Services, actionable market intelligence, and venture capital services focused on global SMBs, extending into large enterprise. AMI's team of analysts and consultants boast strong functional experience in management and strategy consulting, business planning, market research, logistics, marketing and channel distribution, branding, venture investments, alliance partnerships and acquisitions. For more information, please go to www.ami-partners.com