

## **Network Box white paper: Return on Investment**

Threats from the internet are increasing and, as a result, a growing number of large companies have turned to managed security services as a cost-effective way of providing the expertise needed to keep these threats at bay. The decision to outsource security management to experts is taken by large organisations that have done the maths and recognise that it offers the best overall return on investment, protecting both the business and its customers from the disruption and cost of a security breach.

Often, these services have, in the past, been considered to be out of reach for many smaller companies, with the result that they've managed their security in-house. Also with the growth of IT in business processes, even small companies now find significant costs attached when a breach occurs. But as the use of internet and technology for business grows, it just isn't possible for a smaller business to provide the sort of level of service or expertise in-house that can be provided by a specialist. There is now a strong ROI argument for smaller businesses to use a managed security service, which now comes at a price they can afford. For instance, the benefits of consolidating applications onto a single managed appliance means that the managed security service provider is able to reduce overheads in terms of hardware, software and training which can be passed on to the customer.

The figures will vary from company to company, and we leave it to the individuals within those companies to calculate the financial savings gained from using a managed security service. In this document, we will examine the business gains from a managed security service. Firstly, we look at how companies should consider the return on their total investment when comparing the cost of employing security experts in-house (or expecting a non-specialist to manage security systems) to secure their network. This includes not just the 'hard costs', but also efficiency gains of resources to the business – particularly important at a time when technology is becoming of strategic importance to business. Finally, how does the company win in terms of decrease in risk by using specialists?

### **The advantages of Managed Security Services**

There are a number of straightforward advantages in using a managed security service (MSS). The first is speed of deployment. For example, if you're rolling out a new application to be used by employees across the business, your security system will need configuring to allow it to work effectively. Using a managed service, it is possible to deploy the new security system rapidly, from the minute a new application is installed, through to adding new features and new users.

The MSS provider will know these applications inside out. This means they can configure security to allow the application to be used from the moment it is installed, through to adding new features and new users as required. They can help with the installation, set user policies and access rights to make sure the application is used correctly (and securely) by employees. It is our experience that security breaches or network downtime is often caused by mis-use of applications – for example, switching off firewall protection to allow an application to function – because the company doesn't have the technical knowledge in-house to run them in conjunction with other systems, including security.

Knowing an application inside out has another practical – if less technical – benefit for a company. It is less likely to be left in the box for months while the internal IT team struggles to find the time to read the manual, let alone install and test the system before it goes live. Another saving is in the reduced workload on the customer's IT staff – freeing up their time to focus on supporting the business - as many of the routine and time-consuming tasks are taken on by the MSS.

With a well-constructed solution, organisations can implement the managed security service bit-by-bit, increasing the service cover as their existing licences run out or hardware becomes obsolete. Beyond the initial deployment, an MSS also makes it easy for organisations to roll out new users, new sites and new functionality: all the back office work – testing, set up and configuration, for instance - is done by the service provider, so the business just has to switch on new features as they need them. It is the ability to do this quickly that is the real cost benefit over an in-house, do-it-yourself solution.

### **Increased User Adoption**

Often, Customer Premise Equipment (CPE) comes with a huge amount of functionality that for the most part, remains unused. Either the on-site personnel do not know about this functionality or do not have the time to investigate, test and deploy new features that could benefit them. MSS providers will know the equipment and support a company in using all the relevant features greatly increasing return on investment. The MSS should also deliver reports which mean that organisations can more easily identify the areas on which they should focus.

### **Reduced Support Needs**

The technical support in-house that is traditionally used to fix bugs and patch vulnerabilities is usually eliminated completely, as routine tasks are taken over by the MSS provider. This has the advantage of freeing up the IT team to focus on more strategic projects to support the business that they are uniquely qualified to do.

Part of the advantage of a managed security service is that its equipment will be specifically designed to work together, without the usual conflicts and bugs that come from deploying equipment from different manufacturers. This avoids the issues of reduced productivity, downtime and security vulnerabilities.

### **Implementation Costs**

Organisations should factor in significant additional upfront time and cost for a new do-it-yourself deployment. A good MSS provider will be on site with a preconfigured device or devices that only need minimal changes to be deployed, saving engineer time and downtime for the company as a whole.

### **Fixed Costs**

The basic recurring cost for the MSS provider is the subscription cost. This is a fixed annual fee that allows organisations to plan their spend. There is also a minimal cost to the organisation in terms of human resource in administration and support for the managed service. In our experience, the overall cost is reduced by a factor of anywhere between 20 and 40 per cent by comparison to do-it-yourself deployment; however this can vary greatly depending on characteristics such as the type of application, the size of the deployment and the makeup of IT skills in the organisation.

Other costs that must be considered when comparing the cost of in-house staff versus MSS is the training that an in-house team needs to do their job effectively. This can be general

security training, learning about best practice and keeping up with the latest threats, down to the training required to efficiently manage an application or appliance. When using a managed service, this cost is held by the service provider.

The other cost of maintaining skills in-house (that is frequently overlooked) is that of retaining staff, and the cost of replacement when needed. High calibre staff will need to be kept engaged and low quality staff will have to be dismissed and replaced: all expensive exercises. Outsourcing the routine management of security service will often have a positive impact on good staff, who can focus on strategic business IT support, and leave the day-to-day configuration and management to experts.

### **Upgrade Costs**

MSS solutions typically offer seamless automatic, frequent upgrades as part of the ongoing subscription charge. Because these upgrades happen more frequently, and therefore incrementally, than for do-it-yourself solutions, they typically have significantly reduced testing and end user acceptance and training costs.

Organisations rarely have to engage third party consultants the way they would with a major do-it-yourself upgrade.

### **Conclusion**

The key factors that affect whether using a managed security service will be a long term win include the ability to reduce or eliminate IT support/staffing, upgrades, monitoring, change control, backup, on-site replacement and software maintenance. There are additional benefits in terms of reduced training cost and time; and the ability to scale the subscription to remove or add features as the organisation requires

**For more information on securing your company network, visit**

**<http://www.network-box.co.uk>, or  
call James Mackie on 0800 107 6098**

**To keep up with news from Network Box, see Simon Heron's blog:**

**<http://blog.network-box.co.uk>; or follow him on Twitter:  
<http://www.twitter.com/networkbox>.**