Global Information Assurance Certification Paper

Avoiding the Pitfalls of Security Outsourcing

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b

Option 1 , Research on Topics in Information Security

Submitted by Dan Rivers 08th September 2004
Location: GIAC Security Essentials,
London, June 21st-26th 2004

Abstract
The purpose of this paper is to highlight some of the misconceptions of IT security outsourcing, and the areas that need to be addressed if you have, are or are intending on taking this route. My intent was not to write a definitive guide to security outsourcing, but to help identify what can and can not, effectively be achieved by outsourcing your security requirements.

This paper is high level non-technical paper; its purpose is to aid the reader in identifying risks associated with the outsourcing of IT security requirements and provide methods to assist in mitigating against those risks.

My approach to this paper was to look at the feasibility of a completely outsourced security environment. Although my results attempt to demonstrate how it would be impossible to achieve a fully outsourced IT security environment, in doing so I hope to present the reader with a realistic view of what is achievable, and provide the reader with options and choices, enabling him / her to either review their current outsourced arrangement or to assist in planning a new one.

Contents

Contents....1
Why consider Outsourcing....2
Choosing a Managed Service Security Supplier....2
    How to choose your MSSP....3
    The business partner route....3
Common Interpretation of Standards....4
Defining the scope 6
    MSSP provided due-diligence....6
    You provide the due-diligence....6
    The middle ground....6
MSSP Access....7
    Controlling Access....7
Device Ownership....8
Managing your MSSP....9
    Reporting....9
    Auditing....10
Business as Usual....10
The Contract....11
Conclusion....11
Biography....12

Why consider Outsourcing

The complexities and diversity of IT security can make working in this area highly specialised. For an organization to implement its IT security policy and standards, it must have the correctly skilled resource for all areas within its IT infrastructure.

Example:-

Certified Checkpoint Firewall Engineers
Certified Cisco Engineers
Security Architects
Software Security Experts
Health checking Expertise
Technical Security Testers
Desk-side support
Server Support
IT Management
Business Controls
Etc.

All of this specialised resource will cost money, in the UK a trained certified security consultant will cost on average £55k per annum ([14] M.Page Int 2004) (approx $100k). Trying to retain all of this resource in-house, and for all areas of your organization can be very costly. If any of the resource subsequently leaves your organisation you are left with the issue of locating equal replacement resource, while trying to minimise impact to your IT infrastructure and business.

This may be one of the reasons that an organization considers outsourcing its security requirements.

As well as the benefits of dedicated skilled resource, outsourcing also opens up a vast amount of knowledge and experience to smaller organizations. Instead of having to hire individual personnel who specialise only in specific technologies, outsourcing opens up an entire pool of specialised personnel to the organization, to which they would not normally have access. However this does all come at a price, but that price can look substantially lower than hiring in-house personnel.

Let's take a look at some of the steps involved with outsourcing and the issues associated with each of them. The approach taken is that of an organization wanting to completely outsource all of its security requirements while reducing cost and still increasing overall security.

Choosing a Managed Service Security Supplier

It sounds easy but it can be very difficult to choose a good security provider, (also know as a managed security service provider MSSP) as there are no industry standard kite marks to go by. This makes the task of choosing your MSSP more difficult, like a lot of things in life, unless you've either had experience with them or had recommendations from trusted parties you can easily be led astray.

How to choose your MSSP

If you were buying a car you'd want to ensure that the company you're buying from is a reputable one. You don't want to discover the company has gone out of business only after your car breaks down. You'd look for well known suppliers, and go on recommendations from satisfied colleagues, friends, or family members. Also there's no point going to a company who only sells 2 seated sports cars, when you need something to transport 2 adults, 3 children, 2 dogs and your shopping.

Your search for an MSSP should be exactly the same, you need to ensure that what the company offers will either meet your needs, or can be retro-fitted to support your environment. Yes there will be time and resource spent on this research, but It will be worth the time and effort to do this research properly. Remember you are going to have to place a lot of trust in any outsourced security relationship.

> Done correctly, outsourcing can help you focus on your core business expertise; but done incorrectly, you can end up spending too much effort and resources trying to make up for poor service from your service provider, which defeats the purpose of the outsourcing effort.

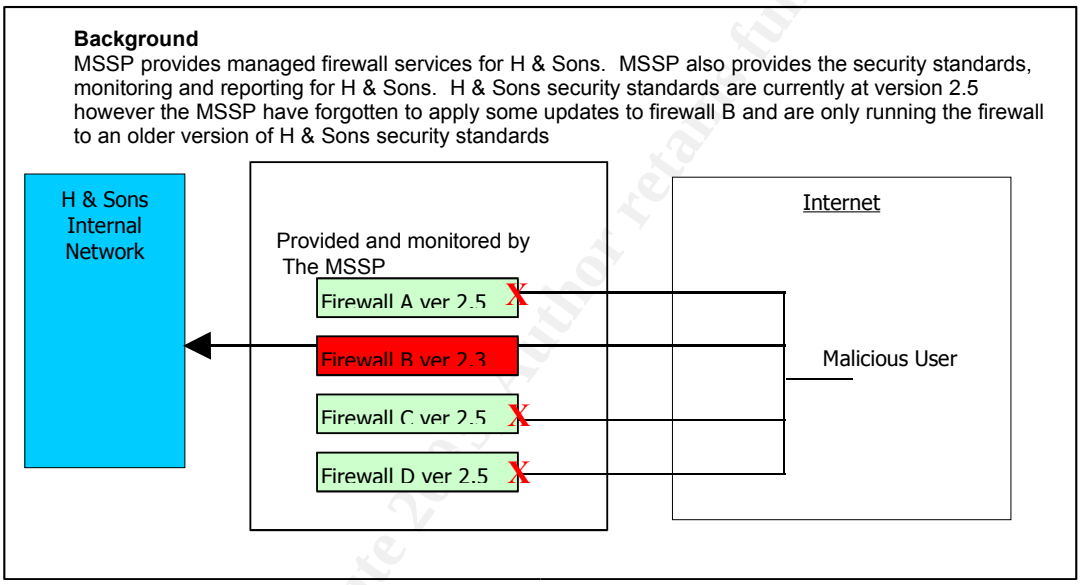
([1] Piedad 2003)

The business partner route

What if you already have an existing business partner / vendor, who can take on your security requirements? You already know and trust them; they're industry leaders in their field, plus you get an additional discount. It's a win, win situation, or is it?

Although the situation looks good there are some real hidden dangers. First and foremost is the conflict of interest. What if your vendor has to ensure security compliance on managed services that they also provide to you? "A service or security mechanism that is provided by a specific company should never be assessed or audited by that same firm." ([4] Huston 2004) How forthcoming would the vendor be if they discover a vulnerability that could cost them money? (See figure 1).

(Figure 1)



(Based on figure 1)
What if a malicious user gained access through firewall B?
As the MSSP provides the support, installation, monitoring and security compliance against this firewall, it would be very easy for the MSSP to cover up the exposure, as it would reflect negatively on them if it was visible to H & Sons.

One of the ways this conflict of interest can be removed, it by enforcing separation of duties. Separation of duties is "The practice of separating functions or roles among different individuals, in order to keep a single individual from subverting a process". ([15] ITSecurity.com 2004). By ensuring that you MSSP does not provide the solution and security compliance / auditing of the solution you are effectively removing the conflict of interest.

If you do choose an existing vendor, the security work that they provide should be clearly isolated from any other contracts that you have with them. Your vendor should be tracked and reviewed against the new security contract only, and a new security relationship built upon this, no other factors should be present. It would be very easy to have a relationship with your vendor based on

good will due to existing agreements, however ultimately you will not benefit from this. If your vendor fails in the security relationship it could potentially lead to a break down in your overall relationship with that vendor.

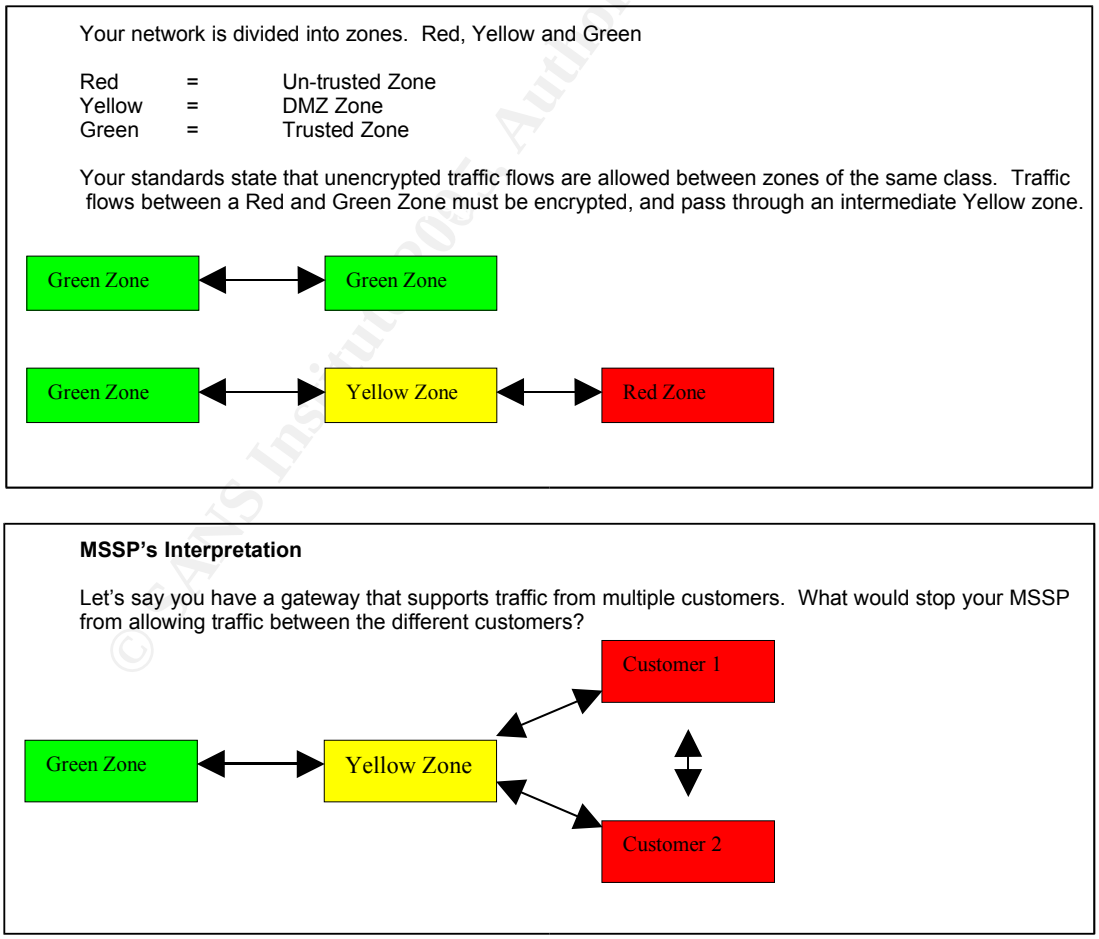
Common Interpretation of Standards

You've managed to find an MSSP that can support your environment, what next? You can't just hand over your security standards, there needs to be a common interpretation of them between you and your MSSP. If your MSSP has a different interpretation of your standards then there is no way that you can effectively meet your organizations security policy.

You can spend millions of dollars; have the best project plan and the best MSSP, but without a common interpretation and understanding of the standards you are not going to achieve the results that you want. You could end up costing your organization more, due to re-architecting work required to fix any misunderstandings. A simple mis-interpretation could cost hundreds of thousands if applied across your entire IT infrastructure.

(Figure 2) depicts a very basic example of a mis-interpretation of an organizations standard.

(Figure 2)



Based on figure 2 your standards state that an unencrypted traffic flow is allowed between zones of the same class. However if customer 1 is able to

see customer 2's data, then not only would customer 2 be less than happy, but you could also be in violation of data protection laws. It is this type of mis-interpretation that could lead to costly legal disputes. Figure 2 is a very simple example, but demonstrates the importance of having clear security policies and standards, and ensuring that you, your MSSP, and your staff all have a common understanding of them.

Policies and standards change constantly, as such this would be an ongoing piece of work. You will have to agree on the initial baseline of the standards, you will also have to ensure that any updates to your standards are communicated correctly to your MSSP. The resource requirement to complete this role would be specialised.

Defining the scope

After you have both agreed on a common interpretation of your standards, both you and your MSSP, need to ensure that you understand what is both in and out of scope of the agreement. If the scope is not clearly defined it could potentially cause contractual issues later.

Our scope will be defined as the entire infrastructure, based on the assumption that we are trying to outsource our complete security requirements. The infrastructure scope can be achieved through detailed due-diligence of the environment that is to be covered by the standards. (As due diligence can mean different things to different people, I am using it in the context of a process to check the accuracy of information). The due diligence in this example is to review all devices within your infrastructure and assess the version of your standards they are currently compliant to. This information will enable you to decide what should be included within the scope of the agreement.

MSSP provided due-diligence

If your MSSP completes this due-diligence, they will require full access to your environment. The due-diligence will generate a complete list of devices your MSSP will be responsible for. Although your MSSP has completed the due-diligence, it will require approval from you as it will become part of the contract agreement.

What if your MSSP has failed to capture all devices within your infrastructure? There is always the possibility of devices being missed; you could of course check the integrity of the device profile, (no easy task if you have thousands of devices) but that is going to require time and resource to complete.

You provide the due-diligence

You provide your MSSP with a list of all devices that you want supported. Again this suffers from the same issue, time and resource has to be spent to complete the task, if any devices are missed your MSSP has no commitment to ensure compliance of them. You could find yourself with non-compliant devices and no resource to fix them.

The middle ground

Both you and your MSSP agree on an initial revision of a device template, this should cover every device required to be in scope of the agreement. A process needs to be established that enables both you and your MSSP, to add, change, and delete from the scope. Any addition, changes, or deletions may affect the contract pricing; if this is the case then revisions, need to be approved by you. You don't want your MSSP adding and changing the scope at will, thus increasing the cost.

The initial one time piece of work could be resource intensive. Due to the nature of the IT environment it is probably fair to assume that this will be an ongoing exercise.

MSSP Access

In most outsourcing arrangement, at some point your MSSP will require access to your environment. This may be in the form of both physical and logical access. This requires careful planning and management.

Controlling Access

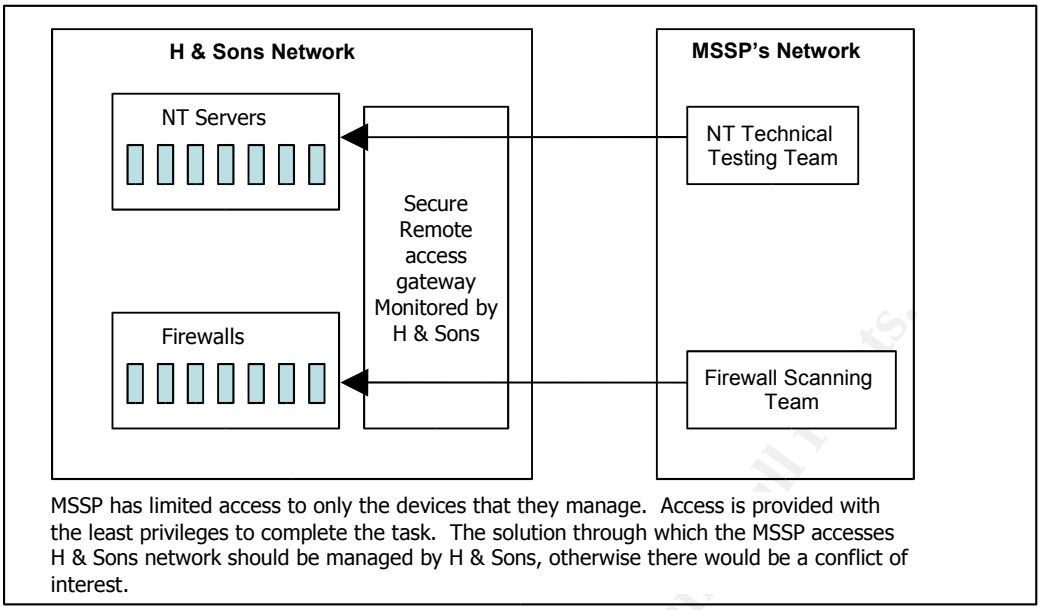
You can't just let your MSSP have free roam of your infrastructure. Access needs to be managed, and least privilege access needs to be enforced. If a team within your MSSP's organisation only provides technical testing, then they should only have access to the components that they need, with the least privileges to complete the task. "You see this all the time in everyday life: You have the key to your office, but not every office in the building." ([2] Schneier p368) This is the basic principle of least privileged access.

If you MSSP requires remote access into your environment, then your MSSP should not be managing the security for the devices that they gain access into your network through. Allowing this would cause a conflict of interest. This role needs to be managed either in house, or by another trusted party.

The same holds true for physical access to your network. Controls need to be in place to ensuring that the person visiting your site is monitored, and only has access to areas that enable them to complete their tasks.

You goal is to limit any intentional or unintentional damage that can be caused to your network by your MSSP just as you would any other vendor.
(See figure 3)

(Figure 3)



We have seen that providing access into our environment means that we still have to monitor and control certain devices; there is no way to get away from this.

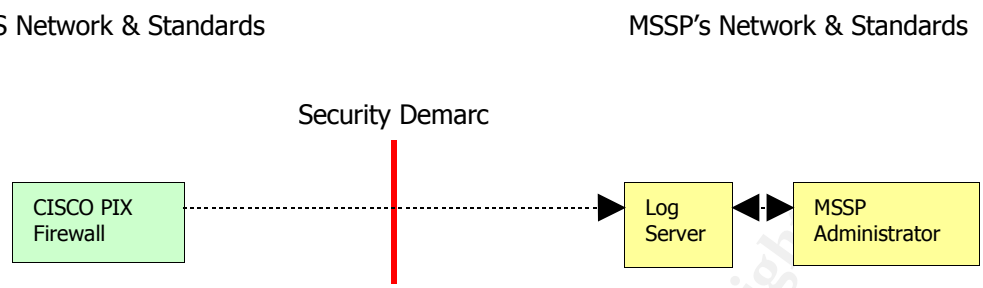
By retaining control of these devices we also own the compliance and security management of them. For example, we need to ensure that these devices meet our corporate standards, have processes that checks for a continued business need (CBN) of MSSP user ID's, and that there is internal executive ownership for the service. All of which needs to be established before any third party access can be granted.

Device Ownership

It may be that as part of the outsourced security agreement and to further reduce costs, certain aspects of your security infrastructure is outsourced as well. For example, log servers, tacacs servers, radius servers, IDS systems, AV servers, etc. In these cases we need to have demarcations drawn up and agreed. See (figures 4 and 5).

(Figure 4)

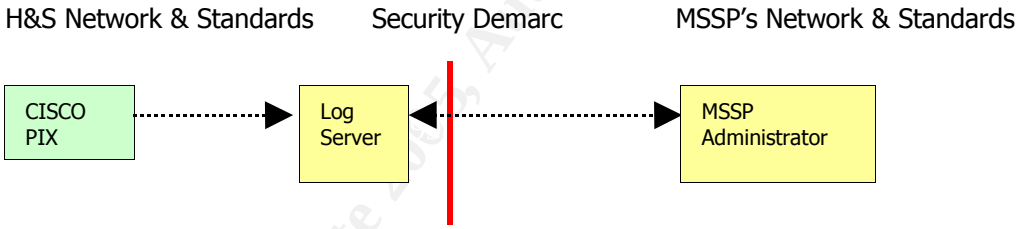
Agreed Demarcations
This shows a Cisco device sending its log information to the MSSP's log server and the MSSP retrieving those log files.



The log server is sat on a network that is not owned by H&S, only traffic is passed between the two organisations. The device conforms to the vendor's security standards and not H&S organisation security standards. The traffic flows still need to conform to H&S standards.

(Figure 5)

Agreed Demarcations
Again this shows a Cisco device sending its log information to the MSSP's log server, and the MSSP administrator retrieving those log files.



This time the log server is sat on a network that is owned by H&S. The log server conforms to the H&S security standards. The traffic flows also conform to H&S security standards.

The demarcation is a logical view of how a device should be treated, regardless of who owns the device. For any devices that support your infrastructure a clear demarcation needs to be drawn up. But why do we need to do this?

Let's say that you have a security incident and have brought investigators into the site to investigate, with the intent of prosecuting the offender. If the log servers that hold the evidence (as per figure 4) are owned by the MSSP and sat on the MSSP's network, then you could have real problems when it comes to retrieving the evidence. Your MSSP's security standards could state that any investigation for devices on their network must be performed by them, and the information must not be exported to third parties. This conflict in standards could cause real problems.

However if the device is owned by the MSSP but sat on your side of the security demarcation (as per figure 5), your standards will govern what information should be held, who should process that information, and what

information should be made available in an investigation. In some circumstances it may not be possible to have a device sat on your side of the demarcation. If this is the case, steps can be taken to ensure that there is a fixed agreement on what can and cannot be requested and made available from that device. Regional law may override certain investigations but the key point here is that in most cases you are maintaining control.

When you are setting up demarcations it is best to try to make them service specific, all implementation of that service should be set-up the same way. This means that the demarcation should be consistent across your organisation globally. This will require a large one time piece of work but should only need revising if services are updated or new services added. Any changes or updates should require minimum resource and effort.

Managing your MSSP

How to we know if our MSSP is actually doing any work at all? We just can't assume that the MSSP is fulfilling all of their contractual obligations. We need to receive some sort of scheduled feedback, and this feedback needs to be managed and reviewed. The more controls we put around this the more control we will ultimately have, however this can be a fine line; we don't want the amount of resource that is being dedicated to managing our MSSP outweighing what it would cost to provide the service in-house. There are many ways to manage our MSSP the following are basic examples.

Reporting

Reporting can be done on a variety of tasks and activities, all of which needs to be clearly defined to ensure that only relevant information is provided. Thought needs to go into what you are trying achieve with these reports, ultimately you want enough information to enable you to feel comfortable about the work your MSSP is completing and its compliance to your standards. You also need to have enough information to allow you to question your MSSP's actions if required.

If there is a requirement to scan devices on a quarterly basis, you would expect at a minimum a report each quarter that show you how many devices were scanned, what findings there were, and what action if any were taken on the exceptions. A good reporting structure will highlight both the good and the bad areas of your network. The ultimate goals of this type of feedback is to put you in a position of control, allowing you to make informed decisions about your infrastructure and its security measures. The type of feedback you receive should allow you to make changes to both your infrastructure and to your outsourced security contract.

When it comes to reporting Jonathan Fieldman's statement pretty much sums it up. "We can't overemphasize the importance of not only collecting the data but making sure a pair of intelligent eyes scans it." ([9] Fieldman 2002). What is the point of setting up an all singing all dancing reporting structure if no one actually looks at it, or worse, the people looking at it don't understand what they are actually looking at.

Auditing

"There is no substitute for vigilant monitoring of security controls" ([8] Harrison 2003). The only way you can be sure that your MSSP is providing accurate reports and running security to your standards is through detailed auditing. This has to be carefully thought-out as any audits will need to be fully articulated in the contract agreement. Processes and procedures need to be in place to deal with any audit findings. Audits can be completed by yourself or by another third party. (However it is normally good business practice to have them completed by an independent third party) The audits need to be completely unbiased and focus simply on both the compliance to your standards and the contract agreement.

This is all part of the day-to-day management of your supplier.

Setting up the management of your supplier is going to take a lot of time and resource, and it doesn't stop there. You will never really know if the management of your supplier is working until you start to see the long term results and data.

Business as Usual

We have covered some of the steps involved when choosing to outsource our security requirements. By now it should be clear that no matter how hard we try we will always have to provide time and dedicated resource when trying to outsource our IT security requirements. We may have moved the resource away from actually doing the work, but we now require resource dedicated to managing the MSSP to which we outsourced to. This new dedicated team has to understand, both the outsourced security contract and our own standards.

Even though we are now at a business as usual stage we still have some potential issues. We know our security standards will change, and we know that a process needs to be in place to enable our MSSP to adopt the new standards.

This raises the question of time frames to implement new standards. What if during the initial negotiations of standards 1.1 the company release standards 1.2? Do you scrap your initial negotiation and proceed with the new standards? If you do this you may never actually get to a stage where you are implementing anything. You can of course complete your initial standards then move onto the newer ones, but depending on the implementation time frames, this could turn into a constant churn or work where you are always 1 step behind the company policy and therefore always non-compliant to your corporate security standards.

As part of the contract agreement strict time frames for delivery of any new standards need to be agreed and enforced. This will mean that a slick process will need to be in place, ensuring that new standards are provided to the MSSP and all pre-requisites are completed to allow work to start. The business as usual stage will require constant support from your organization, the amount of resource will depend on the size of your organizations infrastructure and the level of control that you wish to maintain.

The Contract

Everything should now be in place, we have all bases covered. Everything is agreed, the contract is signed; our MSSP is running our environment to our standards and providing costs to update to our newer standards.

But what do you do if your MSSP fails to meet those time frames?
What if your MSSP has constant audit findings and does nothing to correct them? You tell yourself that you should be ok as you have everything documented in the contract agreement; we know what is in scope and what is not, and we know what our MSSP must deliver.

That's all fine, but what penalty does your MSSP face if they don't deliver? What if they don't meet the agreed service level agreements? (SLA's) If there are no clear penalties then the worst that your MSSP could face could be no renewal of the contract. If you're in a long term contract, say 10 years or so, this isn't going to help you. There has to be a means by which you can measure your MSSP's performance and renegotiate the contract, say every 12 months or so. These types of short-term contract help keep both you and your MSSP on your toes, ensuring complacency doesn't set in.

As well as renewable contracts there should be clearly defined penalties that ensure your MSSP has the correct focus. This can be a very tricky area, only you can decide on the best way forward for this. Your legal teams should review this with senior management and have clearly defined tolerance levels specified. Again this should be written into the contract agreement.

Conclusion

We have looked at some of the areas that need to be addressed when considering outsourcing your security requirements, this is by no means definitive. However what should be apparent is that we cant just outsource this whole area, we need to provide dedicated resource to correctly manage it. Outsourcing security in not a silver bullet, it won't fix all of your problems. If you approach outsourcing like this then you could be on a path to failure.

I do not believe that IT security can ever be fully outsourced. The reason for this is control. By its very nature security defines levels of control over your environment. No matter what approach we take we must always be in a position of control over our security infrastructure, by correctly managing our MSSP we can still retain this control.

There are benefits in outsourcing pieces of security work as long as you understand the control mechanism that go along with it. Outsourcing specific areas of your IT infrastructure, to an MSSP with those particular skills, may allow you to free up your own resource to focus on the task of actually managing security. However this can be a very balanced and fine line, and must be approached with both caution and a full understanding of the potential risks to your organization. You need a full understanding within your organization, of areas where you are lacking, then asses whether you can gain more control by outsourcing those tasks to a third party. Bearing in mind that outsourcing certain tasks could bring with it, its own inherent risk, and the

actual outsourcing of these areas could well be a deviation from your own standards.

For any organization the deciding factor for outsourcing is a financial one. All too often organizations only see the short term savings. Any decision to outsource should be based on a fully quantified risk assessment. You should always be aware that sometimes the cost and resource of managing your MSSP over a long period of time can far outweigh the cost of actually doing the work yourself.

Biography

[1] Floyd Piedad, http://techrepublic.com.com/5100-6314-1060263.html (2003)

[2] Bruce Schneier, Secrets & Lies, Digital Security in a Networked World: USA: Wiley Computer Publishing: (2000): p368

[3] Bruce Schneier, http://www.computer.org/security/supplement1/sch/

[4] Brent Huston, http://security.itworld.com/nl/security_strat/05252004/ (2004)

[5] Bee Leng, http://www.giac.org/practical/GSEC/BeeLeng_Tiow_GSEC.pdf (2003)

[6] Dan Blacharski, http://www.networkmagazine.com/article/NMG20000426S0026 (2000)

[7] Lauren Gibbons Paul, http://www.darwinmag.com/read/080101/blunders.html (2001)

[8] Reed Harrison http://www.computerworld.com/securitytopics/security/story/0,10801,80167,00.html (2003)

[9] Jonathan Fieldman http://www.networkcomputing.com/1308/1308f2.html (2002)

[10] Scott Berinato http://www.cio.com/archive/080101/exposed.html (2001)

[11] Jonathan S Faile http://www.sans.org/rr/papers/37/223.pdf (2001)

[12] Bee Leng http://www.sans.org/rr/papers/37/1241.pdf (2003)

[13] Nils-Åke Carlsson, Olle Hammarström http://www.union-network.org/Ibits.nsf/5751d24322e603308025646c003b28b8/9e0b613362344979c125667a0033d54d?OpenDocument (2001)

[14] Michael Page International http://www.michaelpage.co.uk/controller?event=VIEW_SUBSECTION&sectionname=perfect_job&sectionid=2&subsectionid=11160 (2004)

[15] ITSecurity.com http://www.itsecurity.com/dictionary/separation.htm (2004)