my redfort community

IT Security as a Managed Service

Considerations for the SME

Ashok Thomas

March 2022

Ashok Thomas, CEO of leading managed security company, NetUtils, talks candidly about the pro's and con's for SME's thinking about taking a managed security service into their business

Introduction

There are many reasons why a business may choose to turn to a managed service for all or part of its IT Security operations. These often include cost savings from owning and managing a cyber security estate and employing enough of the right staff to do so.

With the rapid march towards digital transformation, cost isn't the only reason. Even if a business has an IT department, they may not have the skills or people to keep pace with the exponential rise in cyber security threats.

Taking a managed service for the cyber security aspects of your business both relieves pressure on internal resource and ensures knowledgeable experts are on hand with the right skills and technologies to guarantee service levels.

Managed Security Services provide access to the latest industry processes and techniques to conform to statutory compliance and regulation requirements as well as protecting an organisation's data, customers, staff and suppliers from the ever-present risk of cyber attack.

Here are what we think are the top reasons companies outsource, or partially outsource, their IT Security function.

The Key Upsides:

Reduce and control operating costs

When you outsource, you eliminate the costs associated with hiring an employee, such as management oversight, training, health insurance, employment taxes, pension plans etc.

Improve company focus

It is neither practical, nor possible to be a jack of all trades. A managed service allows you to focus on your core competencies while another company focuses on theirs.

Gain access to exceptional capabilities

Your return on investment is so much greater when you take a managed service in the exact areas you need. Instead of just the knowledge of one person, you benefit from the collective experience of a team of IT security professionals. They come with all the necessary industry training, accreditations and certifications so you don't need to keep in-house staff trained.

Free up internal resources for other purposes

Any internal staff are enabled to carry on with what they were actually hired to do. This allows you to retain your employees for their intended use, rather than spending their time on things that may take them longer than someone who is trained in these specific areas.

Resources are not available internally

On the flip side, maybe you don't have anyone in your company who can manage your IT security needs, and hiring a new employee is not in the budget. Outsourcing can be a feasible alternative, both for the interim and for the long-term.

Maximise restructuring benefits

When you are restructuring your company or undertaking digital transformation programmes to improve costs, quality, service, or speed, your non-core business functions may get pushed aside.

Cyber security is high on the agenda so taking a managed service is an optimal way to manage resource without sabotaging restructuring efforts in other areas.

Function difficult to manage or out of control

This is a scenario when taking a managed service can make a big difference. But don't make the mistake of thinking you can forget about the problem now that it's being "handled." You still need to be involved even after control is regained.

Make capital funds available

By outsourcing non-core business functions, you can spend your capital funds on items that are directly related to your product or your customers, moving your entire cyber security strategy to an operational cost.

Reduce risk

Keeping up with technology required to run your business is expensive and time consuming.

Because professional outsourced IT providers work with multiple clients and need to keep up on industry best practices, they typically know what is right and what is not.

This kind of knowledge and experience dramatically reduces your risk of implementing a costly wrong decision.

The Main Downsides:

Anytime you give someone else responsibility for an aspect of your business, whether a full-time new hire or an outside provider, there's risk involved.

Did I hire the right person/company to do the job? Will they do what they are supposed to do? How will they "fit" with existing employees or departments? These are the questions that bother owners of small businesses when handing over the reins whether it's a new employee or service provider.

IT helps to be aware of the following risks:

Some IT Security functions are not easily outsourced

IT Security affects an entire organisation - from keeping an eye on simple tasks employees do every day such as receiving email, or more complex access rights. Be sure the Managed Security Services Provider is qualified to take care of your greatest needs.

Control may be lost

Critics argue that an outside provider will never be as effective as a full-time employee who is under the same management as other employees. Other concerns include confidentiality of data and disaster recovery

Employee morale may be affected

This is particularly true if you will be laying off employees to replace their job functions with a managed service team. Other employees may wonder if their job is at risk, too.

You may get 'locked in'

If the Service Provider doesn't document their work on your network and system, or if you've had to purchase their proprietary software, you may feel like you can't go anywhere else or take back your network.

Many Service Providers require you to sign a year-to-year contract which limits flexibility.

Most of these risks can be avoided altogether if you know what to look for in an MSSP and ask the right questions.

my redfort community

6 Tips on managing a successful MSSP relationship

ONE: Clearly form and communicate the goals and objectives of your project or business relationship.

TWO: Have a strategic vision and plan for your project or relationship.

THREE: Select the right provider through research and references.

FOUR: Insist on a contract or plan that includes all the expectations of the relationship, especially the financial aspect.

FIVE: Keep open communication with all affected individuals and groups.

SIX: Rally support and involvement from decision makers involved.

How do I find the right fit MSSP?

Once you've decided managed security services could be an option for you the next step is to find a partner which you are comfortable working with. There are many MSSPs to choose from ranging from large 'bodyshops' to smaller, and often more specialised, providers to choose from.

Many offer consultancy services at the outset to help determine your existing requirements and likely future needs which will help you to decide how it needs to grow over time.

A good MSSP will be happy to spend time getting this right and be able to offer the right pricing model to meet your needs.

Should I look for an offshore provider or stay home-based?

Offshore service providers may be able to offer good rates, but there are many considerations involved in choosing to outsource to your cyber security services overseas.

For example, will the offshore services be subject to the same legal and regulatory regime as any onshore services such as data protection, GDPR compliance, ISO standards for data security and quality.?

Who will audit the offshore services, and correct any problems? Also, will the offshore provider have a sufficient degree of familiarity with the language and customs of your users and your customers?

Ensuring that you get the most out of your outsourcing relationship means you will need to have regular meetings with your service provider and measure their performance and targets. With an offshore provider, this could be an issue.

Conclusion:

There's a lot to think about. Whether you choose to take on an MSSP or hire internally, one thing's for certain - you must know how to manage successful working relationships with your external providers.

If that means working directly with vendors or with your chosen Service Provider our 'Tips on Managing a Successful Working Relationship' will help you get the best for your business.

About Ashok Thomas:

Ashok Thomas, Chief Executive Officer, NetUtils

IT industry veteran, Ashok Thomas, has experience spanning some 35 years, 15 of which were at IBM. He founded Metropolitan Networks in 2003, which went on to be acquired by Network Utilities in 2019. He continues to fuel the success of the organisation with his wealth of industry knowledge and business experience.

Ashok regularly shares views and insights for an industry that's evolving at pace and you can find what he has to say here:

LinkedIn https://www.linkedin.com/company/network-utilities/

Twitter @networkutils