THE BUYER'S GUIDE TO MANAGED SECURITY SERVICES

What to Look for and Avoid When Sourcing Managed Network Security

chess®

Introduction

As with all IT services, when it comes to CyberSecurity, businesses and public sector organisations have a choice: manage the whole security piece themselves (perhaps with selective point solution support) or outsource some or all network security management to a MSSP (Managed Security Service Provider).

As with all IT services, when it comes to CyberSecurity, businesses and public sector organisations have a choice: manage the whole security piece themselves (perhaps with selective point solution support) or outsource some or all network security management to a MSSP (Managed Security Service Provider).

Taking the MSSP route is increasingly popular given the fast-evolving sophistication of blended threats and the GDPR regulations bringing stringent requirements for safeguarding of data.

Avoiding data breaches is now seen by many organisations as the number one IT imperative after operational continuity.

There are many benefits of outsourcing CyberSecurity requirements to a MSSP, but the process is not without its complexities. Selecting the right partner can bring multiple benefits; equally making a poor decision can lead to catastrophic consequences.

In this Chess Whitepaper we will explain the reasons you might consider going down the managed security services route and the potential benefits of doing so. We'll also present a framework for how to assess and evaluate potential providers, including track record, skills, people, processes and technologies.

Whatever the reasons you are considering working with a MSSP, we hope you will find this Buyer's Guide to Managed Security Services a useful tool in your decision process.

Why Use a Managed Security Service Provider?

Many analysts agree that a MSSP should be able to combine CyberSecurity technology, skilled and experienced staff and process management capability to maintain security continuity as unobtrusively as possible.

After all, CyberSecurity is not an operational process in itself; it's there to support business processes and to ensure that — through a blend of preventive measures, continual monitoring, threat detection, proactive and automated updates and rapid incident response and remediation — it helps keep your business operational whilst your employees focus on their core roles.

Most organisations choose to work with a MSSP for one or more of the following reasons:

- A shortage of available (or affordable) in-house CyberSecurity skills
- The scale and complexity of CyberSecurity technologies required
- The speed with which the threat landscape changes and the need for 24-7-365 protection
- Budgetary or headcount constraints
- A business preference to outsource what can best be delivered by a specialist provider.

Underpinning all of these reasons for outsourcing to a professional MSSP is one main factor: the speed with which new attack formats, vectors and vulnerabilities develop and evolve is increasing all the time, meaning that internal IT teams are finding it increasingly difficult to keep up.

Once a network security solution is installed and deployed, it invariably requires management, including immediate updating. The myriad sources of and automated methods used by hackers, means that counter measures must be agile and responsive round the clock.

It's a highly resource-intensive effort to stay ahead of cyberthreats, using data such as event logs and security intelligence feeds from multiple resources to adjust, update and manage security defences constantly.

Among other reasons for hiring a MSSP, they:

- Work around the clock because data breaches don't only happen in business hours
- Provide a range of integrated services, expertise, technologies and processes
- Enable your business to maintain compliance via analysts who monitor the wider industry and compliance/regulatory landscape
- Can help keep CyberSecurity a high priority among C-level executives
- Ensure that your organisation maintains a highly risk-averse position on CyberSecurity
- Transform CyberSecurity expenditure from a 'responsive' to a 'predictable' cost model
- Provide flexible and scalable access to dedicated CyberSecurity professionals who have the necessary skills, experience and accreditations
- Free up internal resources to focus on core operational business functions
- Free up internal CyberSecurity resources to focus on elements of network security that may be best managed in-house
- Can detect and respond to cyberthreats and attacks as soon as — or before — they arise, thereby minimising network downtime
- Can integrate and manage technologies from multiple security vendors to provide a consolidated CyberSecurity solution
- Obviate the need to set up an in-house security operations centre (SOC)
- Improve overall operational efficiency by outsourcing 'enterprise level' security to security professionals

Discovering Your Organisation's Current CyberSecurity Posture

Before you set out to find a MSSP, it's important that know why you are doing so and what you are looking for. Getting the requirements brief right at the start will help you find the right supplier.

A MSSP can manage many different aspects of your CyberSecurity, from anti-virus updates to full time in-house or remote services via the cloud. Some MSSPs specialise in a specific aspect of security such as firewalls or security solutions from a specific vendor. Others may be able to deliver a fully integrated suite of vendor solutions.

Which is right and best for your organisation?

All forms of MSSP have their merits, so what matters is your organisation's needs and current risk profile. What also matters is your attitude and stance to risk and your attitude to outsourcing the management of that risk (see Migrating to Your New MSSP).

Given the importance of CyberSecurity, it is vital to find a MSSP that is a good fit for those needs. But how is your organisation currently positioned to take on a MSSP in the context of its attitude to giving up full or part control of such a key operational area?

A MSSP can manage many different aspects of your CyberSecurity, from anti-virus updates to full time in-house or remote services via the cloud.

Start by asking a few questions about your current situation

1 Why do we need a Managed Security Services Provider?

When you start out on the journey to sourcing a MSSP, it's vital you know what your end objective is, and why you're considering the MSSP route.

2 How are we doing at the moment?

From a CyberSecurity risk management perspective are you:

- Stretched to the limit, hoping and praying things will be OK?
- Just about coping, but with a team that's overworked and understaffed?
- Managing day to day but with a recognised need to improve on several levels?
- Cruising along beautifully well with everything under control?

3 Which parts of our security services do we need to outsource?

Do you want to outsource the entire security function? Or supplement existing in-house security capabilities with bought-in skills to fill a gap?

Think about whether there are parts of your IT set up that require specific or specialised skills and processes, perhaps because of sector regulations. Are you looking to outsource what you currently do, or bring in additional security measures? As well as the 'usual' IT security functions like antivirus and antispam, consider how you manage:

- CyberSecurity threat monitoring and response
- Business-wide software updates
- Firewall policy management
- 24-hour server monitoring
- Compliance
- Operational continuity and back ups
- Data protection
- Specialised functions such as penetration testing

4 What's our position on outsourcing?

Looking back at your track record, it's important to understand whether your business is 'good' at outsourcing.

With IT security there is inevitably a lot of 'letting go' that has to be done — but of course this requires trust in the partnership. So before taking the plunge ask the questions:.

- Do we work well with 3rd party providers?
- Do we feel we can entrust such an important function as our IT security to a 3rd party?
- Do we understand the risks?
- More importantly are we persuaded of and bought into the benefits — right up to board level?

5 How will we work with our new MSSP?

There are numerous ways that organisations can work with a MSSP and the route you choose should depend on your specific requirements. Think about the following options:

- Remote — can our IT security infrastructure be managed remotely?
- On-site visits — do we need on-site visits?
- Support — do we need 'on-tap' IT security expertise, via a helpdesk service?
- Fully managed — do we want our MSSP to supply, install, deploy, update and manage all our IT infrastructure, as well as providing a helpdesk service?

6 How security savvy are our employees?

As we've said elsewhere, protecting your organisation against cyberthreats is not the sole responsibility of your IT department or MSSP partner.

Employees must be educated to take responsibility and be accountable for safeguarding their own data along with access to company data. Knowing how savvy your employees are in this regard will inform your decision on using a MSSP.

Selecting and Appointing Your Provider

When you select your MSSP you need to know what questions to ask and how to evaluate the answers.

Throughout the process you'll need to decipher the truly important information from the 'gloss' that is inevitably used in these situations. The following pointers will be useful in helping to separate the wheat from the chaff.

Price

Number one rule: you get what you pay for. Do not buy on price alone. Look for competitiveness and value-add over price. Expect to pay a fair price, one with which both parties are happy. That way you'll get sufficient focus from your MSSP to ensure their commitment.

Fit with Your Business Objectives

Assure yourself that your potential MSSP has the vision, standards, systems and culture to help you achieve your business goals. Use the evaluation process to ask questions and get a feel for whether the MSSP has an understanding of – or at least empathy with – your strategic business objectives.

Rip and Replace or Adapt?

Ideally you don't want a MSSP that is going to come in and start ripping out your existing technologies to replace them with their preferred solutions. Make sure they'll be happy to see through existing technology to EOL and to adapt it where possible..

References and Case Studies

Any MSSP worth its salt will have plenty of clients willing to say nice things about them. But don't be happy with just a written testimonial. Speak to some of their clients – old and new – about their experiences of your potential MSSP as a supplier.

Service Level Agreements

If enshrined in the contract an SLA ensures both parties understand what is expected. The SLA acts as a guarantee of minimum service deliverables, or if service levels fall below what is expected, the penalties. In some cases (such as a data breach) the SLA may make provision for damages.

Transparency

Using a MSSP is a business decision, so the decision process should not be confused by technical jargon. Your MSSP should be transparent in the language they use and in how they handle the data and processes which they will manage for you.

Know and Understand What You Are Getting

You must be absolutely satisfied about what you are paying for. Everything that you need and that your MSSP commits to provide should be documented in your contract. If it's not there, do not expect to get it once you sign. If you're unsure, ask questions and expect crystal clear clarification.

Skills, Qualifications, Certifications and Awards

Does the MSSP invest in ongoing training and development of its engineers? Similarly, do they have the right numbers of staff with the appropriate certifications to deliver the security support and management services they are committing to? Do they have any partner awards?

Systems and Processes

Find out about the technical support and management systems, processes and technologies your MSSP uses, and whether they have procedures in place for regularly reviewing and updating them. Ask to see procedure documentation and explanations of how and where your data will be stored.

Threat and Breach Response

Understand what steps your MSSP will take in the (unfortunate) event that your organisation suffers a data security breach or a hack. If they've dealt with them in the past, find out what happened and how they addressed the problem.

Partnerships

To support products from a range of security technology vendors, your MSSP needs partnerships with those vendors. Find out as much as you can about how these work, and at what level. The quality partnerships enjoyed by your MSSP will directly benefit your business.

Scalability and Flexibility

You need to manage your IT security within the bounds of your budget, and this will be dictated by the overall performance of the business. If you need to throttle back on certain services, or conversely, to scale up your security programme due to growth or acquisition, you need the flexibility to do so.

Added Value

As well as reporting data metrics and statistics, will your MSSP provide interpretation to allow you to make business decisions? Proactive advice backed by research and investigation is a good example of how a MSSP can add value beyond just the 'operational' service.

Financial Stability

Ask your MSSP to provide evidence of their financial position to satisfy yourself that they're in a stable position. If their business failed, your organisation's security posture may potentially be at risk — and the consequences could be serious.

Migrating to Your New Managed Security Services – What to Expect

Best practice — once you have selected your new MSSP — is to develop a phased and manageable approach to migration.

Why phased? The scale, complexity and risks involved in migrating your CyberSecurity systems management to your new MSSP are all considerable.

So it is best to make the migration phased and gradual, operating a number of key areas in dual mode to begin with.

Your new MSSP needs to add value and implement best security practices for your organisation, but at the same time you may have established policies and procedures that are key to your operations and business sector. They should work around your organisation rather than simply imposing a blanket set of new rules and procedures.

Finally, make sure you have a fall-back position and can take back control if things don't work out. It's not pessimistic to operate like this. It's simply good practice.

> *Your new MSSP.... should work around your organisation.*

Conclusion

In summary, sourcing a new MSSP can be a precarious process.

We hope that with this guide you'll find a few ways to evaluate and assess any new relationship you might be about to enter into.

Ultimately, if you narrow your choices down to a shortlist of MSSP partners, our top 5 points with which to evaluate them would be:

- Expertise/capabilities
- Flexibility
- Price
- Track record
- All round fit for your organisation

You'll get a strong feel for whether it's going to work during the process.

We hope you will choose wisely!

Speak to our team of experts...

Call us now **01284 788 900**
or email **enquiries@chesscybersecurity.co.uk**

---

chess®