LATEST THINKING

Leave security to the experts:

Why a managed security service makes strong business and financial sense

The evolution from outsourcing to managed services

From as far back as the 1980s, organizations have been trying to improve competitive advantage by focusing on their core business while identifying processes that could be outsourced to third parties. Initially these were processes that, while essential, were not associated with the core business - a printer outsourcing fulfilment services for example. The general feeling back then was that the less important services could be outsourced, but it made better business sense to hold onto essential core competencies. That all changed in 1989 when Eastman Kodak decided to outsource the technology systems that underpinned its business. For the first time, a core function was outsourced precisely because it was so important.

Today, cybersecurity is a core business function that is increasingly outsourced to experts, for the same reason. It's too important to leave it to chance or to under-resourced internal teams. The reputational, financial and regulatory repercussions of getting it wrong are too damaging for businesses to contemplate, and it's more than just outsourcing a commoditized service. It's a function that is being increasingly outsourced to specialist managed security service providers who offer a 'management' service rather than a 'deployment' option. And a successful service relies on a partnership between the client and the provider.

This paper looks at why outsourcing cybersecurity management is on the rise and what you need to consider when selecting a service provider.

Digital transformation security challenges

These are challenging times for security professionals and as organizations become more digitally enabled, IT teams are facing security challenges they may never have seen before. The drive to go digital added to an evolving threat landscape, an increasingly regulated workplace and a multi-vendor security environment means updating and maintaining a complex and sprawling security architecture. And that's leading many organizations to revisit their security requirements in order to create an environment that's secure, while also allowing them to evolve and develop their core business.

Outsourcing makes financial sense

With a new approach to cybersecurity required, one question that all organizations need to ask themselves is whether their IT department can reliably and cost effectively manage all cybersecurity related priorities in house. Or would it be more effective to outsource security to a specialist Managed Security Service Provider (MSSP) and move towards a more predictable operating expenditure model? Cost is always a consideration for IT and procurement teams and a common misconception is that engaging with an MSSP would be more expensive than hiring your own staff to manage security.

A managed security service provider (MSSP) provides outsourced monitoring and management of security devices and systems. MSSPs use high-availability security operation centers (either from their own facilities or from other data center providers) to provide 24/7 services designed to reduce the number of operational security personnel an enterprise needs to hire, train and retain to maintain an acceptable security posture.

Gartner IT Glossary: What is an MSSP?

In fact, research by NTT Security[1] highlights that 33% of organizations with no plans to use an MSSP cite cost as the reason. Yet, 23% of organizations that do plan to use an MSSP believe that it's cheaper to outsource. It's rarely the case that MSSP costs will be higher than your own resourcing and operating overheads. An MSSP will share its resources across more than one client and agree a service level with each. Hiring your own team is less flexible, with fixed salary costs and overheads to consider, and the onus is on your organization to fully utilize the team. It's also the case that a good MSSP will have extensive knowledge and professional relationships with security solutions vendors; relationships that they will leverage on your behalf as part of your service agreement. The NTT Security research shows that 29% of organizations planning to use an MSSP would do so to gain access to better technology, and 16% of people need

help with cloud migration and digital transformation.

Do you have the requisite security skills in house?

A global lack of cybersecurity skills has been well documented in recent years. According to a global survey[2], the number of unfilled cybersecurity jobs globally will rise to 1.8 million by 2022, a 20% increase from 2015 estimates. The same survey of 19,000 cybersecurity professionals worldwide, found 66% of survey respondents (up from 62% in 2015) feel they do not have enough employees to address increasing levels of threat.

For now, that leaves a widening gap in the number of IT security experts needed to manage a greater number of threats. And security sprawl is adding to the challenge globally – with a growing number of security technology products and an increasing number of security vendors to manage.

Engaging with an MSSP means that organizations have immediate access to experienced, trained cybersecurity professionals without making the considerable investment in hiring, training, paying, and retaining an in-house team. This allows the business to free up internal resources to concentrate on IT strategy and planning, leaving the MSSP to provide continuous security monitoring 24 hours a day.

The research results from NTT Security's Risk: Value 2018 Report support this too - with 20% of organizations citing a lack of internal resources or a lack of internal skills (18%) as a reason for planning to use a third-party managed security services provider.

Governance, risk management and compliance

Regulatory change is happening on an unprecedented scale and managing compliance is a complex, time consuming, and evolving challenge for organizations in all sectors around the world. Some industry sectors have more compliance challenges than others, particularly financial services and healthcare, but whichever sector you operate in, there will be compliance issues to manage. Non-compliance can cost a company dearly.

The General Data Protection Regulation (GDPR), for example, allows for steep penalties of up to **EUR 20 million or 4% of global annual turnover, whichever is higher, for non-compliance.**

Furthermore, reputational damage as a result of regulatory non-compliance can damage both your brand and your bottom line.

Understanding your compliance obligations, effectively filling compliance gaps and streamlining audits is essential to avoid huge fines and a good MSSP can help with this.

Timely threat intelligence

Threat intelligence can play a crucial role in protecting a company's assets and staying one step ahead of potential losses, providing companies with actionable information that they can use to detect and respond to emerging and evolving security threats. A recent Ponemon report[3] highlighted that 84% of organizations indicated threat intelligence is 'essential to a strong security posture'. Yet, many organizations struggle with an overwhelming amount of threat data and lack of staff expertise, which diminish the effectiveness of their threat intelligence programs. An under resourced IT team, while understanding the value of threat intelligence and early threat detection, will be swamped by the volume of threat data. An MSSP with a dedicated cybersecurity team is in a better position to provide timely threat intelligence, faster threat detection and a prompt response to attacks as they happen. And with some MSSPs operating globally and specializing only in security,

[1] *NTT Security Risk: Value 2018 Report*

[2] *The 2017 (ISC)^2 Global Information Security Workforce Study, Frost & Sullivan*

[3] *The Second Annual Ponemon Study - The Value of Threat Intelligence*

their focus on monitoring the global threat landscape is significantly more effective than that of an internal IT team with myriad priorities.

Selecting a managed service partner

For those organizations that come to the conclusion that some security services would be better outsourced, the next question is what do you outsource - and who do you choose to provide that managed service?

There are a number of MSSPs to choose from in this fast-growing space, but it's worth remembering that you're looking for a long-term partnership here. You're not outsourcing a mailing fulfilment, but a business-critical function, and you'll need an organization that works as an extension of your own team.

As part of your decision-making process, establish a few ground rules and ask some detailed questions before you make your choice:

- **Security expertise** - does the MSSP have the domain and security expertise needed for your specific environment? With today's global lack of cyber skills, be sure that you are employing a partner with access to the brightest talent.
- **Global reach** - Global MSSPs should be on your short list from an evaluation perspective. They see more current and advanced threats and will be in a position to respond quickly when your business is threatened.
- **Technology** - MSSPs rely on either proprietary or third-party technology to examine device logs. Consider service providers that have purpose-built technology for managed security services with advanced analytics to detect sophisticated threats.
- **Remote and on-site support** - does the MSSP offer both? While remote support helps resolve small issues quickly, there's no replacement for in-person contact with your IT professionals.
- **Customer experience** - check that the MSSP can tailor its service to the specific needs of your organization rather than offer a one-size-fits-all approach to managed security services.
- **Cost efficiency** - can the MSSP provide a flexible solution to align with any budget constraints?
- **Experience** - there are many newcomers to the MSS space. Established providers have gained years of experience, refining their technology and processes along the way.

Benefits of a relationship with an MSSP

Lower costs – staffing your own security team for 24/7 security coverage is expensive, as is continuously hiring, training and retaining new staff.

Coverage – monitoring your own networks round the clock, 365 days a year can be cost prohibitive.

Hiring experts – there's a global shortage of cyber skills. With an MSSP you're hiring a team of security experts with access to the latest thinking, up-to-date technologies, and industry expertise.

Shared experiences – an MSSP will draw intelligence from its wide customer base, so you will benefit from the breadth of its reach.

Security focus – if security isn't your focus it can be a distraction and a drain on resources. Focus on what makes you money and leave security in the hands of experts.

Threat intelligence – huge data volumes will overwhelm you An MSSP will provide timely and actionable threat intelligence, accurate threat detection and a prompt response to attacks as they happen.

Global reach – an MSSP with operations across the globe will have access to global security operations centers (SOCs) and visibility to an extensive threat landscape that would be impossible for you to replicate.

Disclaimer: The work described in this thought leadership was performed while the company was known as NTT Security.

NTT