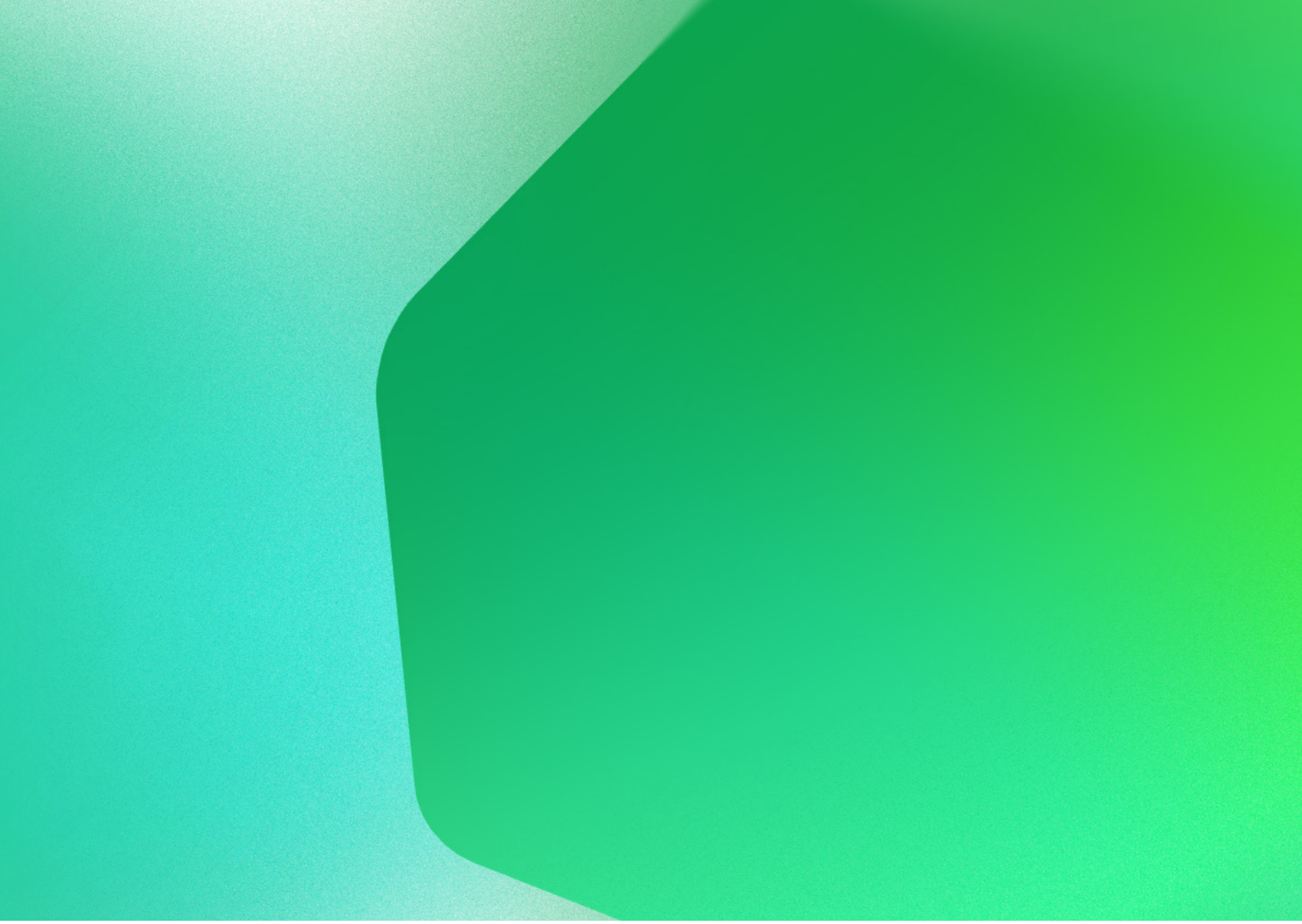

Maintaining MSP Momentum: Challenges and opportunities in an evolving IT security landscape

kaspersky

Contents

Introduction

The managed services provider (MSP) market is big business. What started as essentially an IT reseller role, to provide, install and manage a specific application, has evolved into MSPs becoming an integral part of a company's IT provision and support network. For many businesses, an MSP is an extension of their IT team – or in some cases is their IT team – often making up the shortfall in skills and resources which are lacking internally, to ensure IT operations run smoothly and successfully.

SMBs, in particular, rely on MSPs to be their trusted adviser as the IT landscape evolves, and internal skills and budgets often restrict their ability to keep up. The continued, predicted growth in cloud services is just one example of where MSPs play an important role in helping smaller businesses take advantage of cloud-based applications.

With Gartner predicting that the worldwide public cloud services market will grow 17.5% in 2019 to total $214.3 billion, there is a great opportunity for MSPs to help companies make these projects a success. In fact, through 2022, Gartner projects the market size and growth of the cloud services industry at nearly three time the growth of overall IT services.

It is therefore no surprise that according to recent figures, the managed services market is expected to grow from $180.5 billion to $282 billion by 2023. This is largely being driven by organizations relying on MSPs to 'boost their business productivity and [meet] growing demands for cloud-based managed services'. Another key reason for this increase is value associated with outsourcing IT and security management.

There is no escaping the fact that malicious cyberattacks on businesses are on the rise, which is making businesses much more aware of the risks and consequences of a data breach or ransomware attack on their business. Whilst many of the publicly-known cases are of big, enterprise-level companies suffering a data breach, smaller companies and those in the supply chain are just as vulnerable and the consequences just as serious.

With technology the backbone of every business – no matter what their size or industry – keeping pace with innovative applications and the evolution of security threats can be a challenge. This is particularly true for those companies without enterprise-scale budgets or resources. In fact, recent Kaspersky research has found that businesses with less than 500 employees are more likely to turn to outsourced service providers to ensure the successful management and security of their IT infrastructures. 40% outsource their IT management, and 33% specifically outsource their IT security, to a third party.

These high figures suggest that with budgets and resource stretched, companies feel the best solution is to get an external expert to help. While this presents a huge opportunity for MSPs – evidenced in the predicted growth of the global market – it also presents challenges and puts huge expectations on providers, to fill the skills gap, as well as take the blame should a company suffer a breach or downtime.

To help understand current challenges and opportunities for MSPs across Europe, this report looks at evolving market dynamics and the impact of changing client relationships and expectations on the MSP industry. It also makes recommendations for MSPs to ensure they can take advantage of the opportunities and maintain long-term relationships with their clients, no matter what challenges come their way.

Key findings

- IT outsourcing – and in particular security outsourcing – is on the rise. A third (33%) of businesses with less than 500 employees in Europe currently outsource their IT security management, with 21% planning to do so over the next 12 months.
- The trend to outsource is largely driven by a lack of internal skills, and companies wanting to make the most out of available IT budgets. Half (51%) outsource to supplement internal skills and 52% feel that working in this way will help them reduce security-related costs.
- When IT budgets are cut, companies lean towards outsourcing as the most cost-efficient way to ensure value and support future IT security management needs.
- Three quarters (75%) of MSPs admit that meeting the demands of clients is a key challenge, with two-thirds (68%) struggling to maintain profitability in customer relationships due to over-resourcing to deal with user-based security issues.
- Market reputation is key to attracting and retaining clients, with 83% of MSPs relying on word of mouth, recommendations, salespeople directly approaching prospects (50%) and event sponsorship (48%) to boost their customer base.
- The same is true when it comes to MSPs selecting a security partner – 92% make the choice based on reputation and price. As with their own customers, to add value to their offering, MSPs need to work with a partner who not only has the right solutions and expertise to support them, but can offer this at the best price point.
- When it comes to expectations from today's MSPs, being an expert in cloud & on-premise infrastructure is the main quality that clients need (84%). Cybersecurity capabilities also featured high on the list, with 74% of clients considering this a key attribute in their MSP partner.
- Dealing with the unexpected can have a strain on client relationships and a financial impact for MSPs, making it harder to maintain revenue growth. Three-quarters (78%) of clients expect MSPs to deal with issues outside of their contract, and 65% of MSPs deal with security issues created by user error rather than related to the services they manage.
- This can lead to MSPs often taking the blame for security incidents which were not a result of their negligence. 43% of companies who have suffered a data breach blamed their MSP, with 27% putting it down to a lack of IT security knowledge by their service provider.

Methodology

The findings in this report are taken from two data sources:

- Telephone interviews conducted in July – August 2019 with 101 MSP employees in the UK, France, Germany, Spain, Italy, Austria, Sweden and Denmark.
- Kaspersky Corporate IT Security and Risks Survey 2019 – an annual, online survey of business IT decision makers conducted in June 2019 across 23 countries. This report focuses on the responses of those working in businesses across Europe, with under 500 employees.

IT outsourcing: changing MSP market dynamics

The European outlook

The role of an MSP for businesses is shifting, from simply providing solutions to becoming a trusted adviser and lynchpin for operational success. As such, outsourcing IT is becoming the new normal, as companies look to the experts to advise and manage their sprawling IT infrastructure and everything that comes with it.

40% of businesses across Europe with less than 500 employees currently outsource the management of their IT to a third party. A third (33%) also outsource their IT security management, suggesting that this is a key area of IT support which companies are now relying on their provider to cover for them.

This is a common theme across Europe, with The Netherlands leading the way when it comes to outsourcing IT security provision (45%), closely followed by Sweden (39%) and Italy (39%). Other countries are however picking up pace, with Poland (35%), The Czech Republic (24%), France (22%) and Spain (22%), expecting to show the most growth in outsourcing their IT security management over the next 12 months.

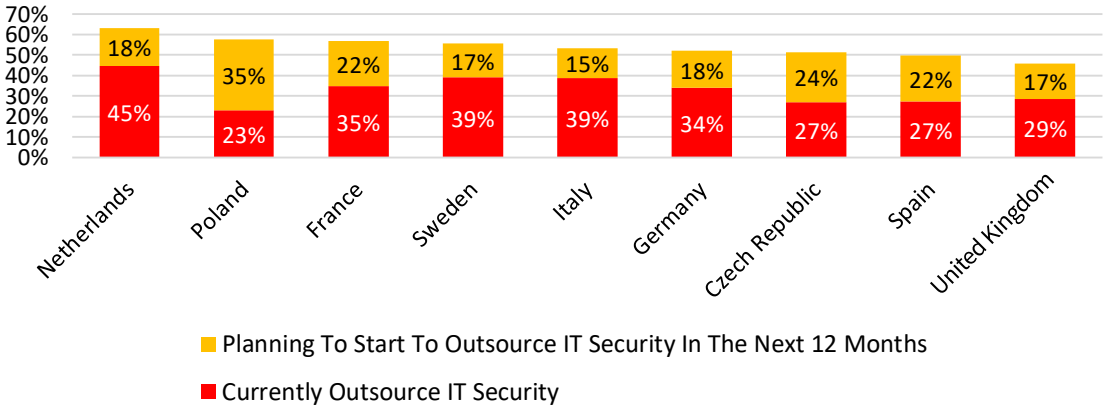

Figure 1. Current levels and expected growth in IT security outsourcing over the next 12 months

For those companies taking an outsourced approach, the engagement model can take different forms, depending upon the specific requirements of the business. The majority of MSPs see their clients wanting a partnership or mixed approach (51%), supplementing internal skills with outsourced expertise for the perfect balance in IT security management. However, almost a third (29%) of MSPs feel that companies prefer to outsource the entire IT function to them, including IT security.

What's driving the decision?

As with many business decisions, cost is the main driving factor behind the need to outsource IT security management. Over half of companies that are planning to outsource IT security management (52%) feel that working in this way will help them reduce security-related costs, with over a third (38%) looking to outsource all IT to a third party – including security – as a result. Interestingly a third (33%) of companies consider outsourcing IT security as a way of ticking the SLA and accountability box. The same (32%) proportion of businesses admit that they simply do not have the internal resources or expertise to provide the necessary levels of security needed for their operation.

On the flip side however, there are reasons why companies chose not to outsource their IT security, which is worth MSPs bearing in mind as they look to grow their offerings and build lasting relationships with clients. Despite skills often cited as the main reason for working with a third party, 40% of businesses that are against outsourcing IT security management we spoke to feel they have sufficient expertise internally to management their own IT security. Another cause for concern for a third of businesses (33%) is the perceived high costs associated with outsourcing their IT security management.

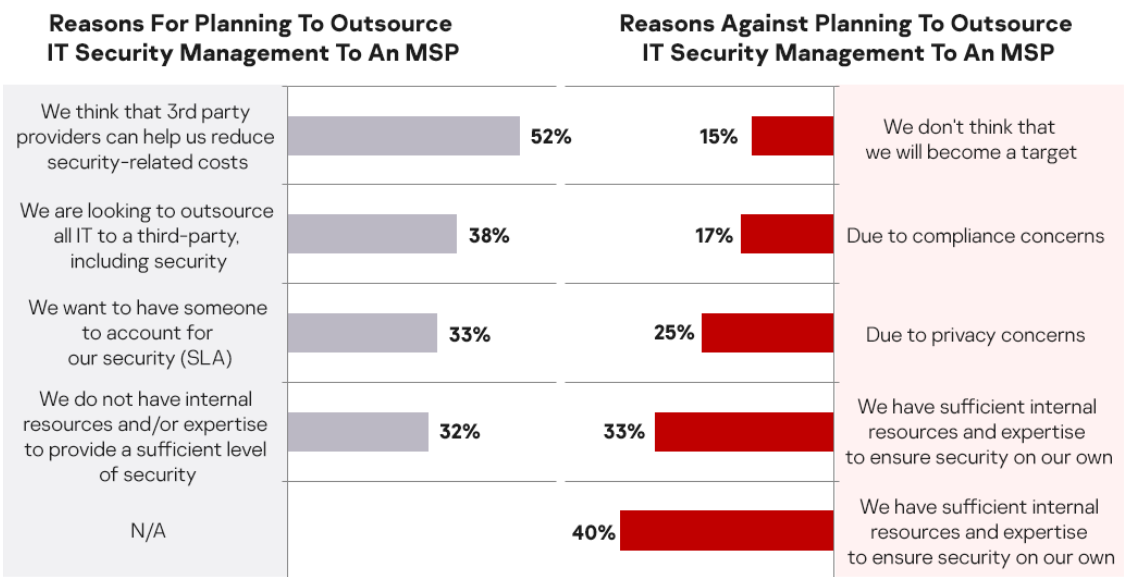

Figure 2. Pros and cons for planning to outsource IT security management to an MSP

A deeper dive into the decision-making process within different industries, shows there are various motivators to outsource. While cost savings are the driving force for most industries, the healthcare sector cites privacy concerns as the main reason not to outsource, with the education sector feeling that the price of third-party solutions is too high.

The cost versus budget conundrum is certainly a challenge for MSPs and businesses to get to grips with. Interestingly, those companies who expect their IT security budgets to increase will invest this in bolstering specialist internal IT staff. However, a decrease in budget would see businesses lean towards an MSP to help support future IT security management, suggesting that they see more value working in this way when budgets are tight.

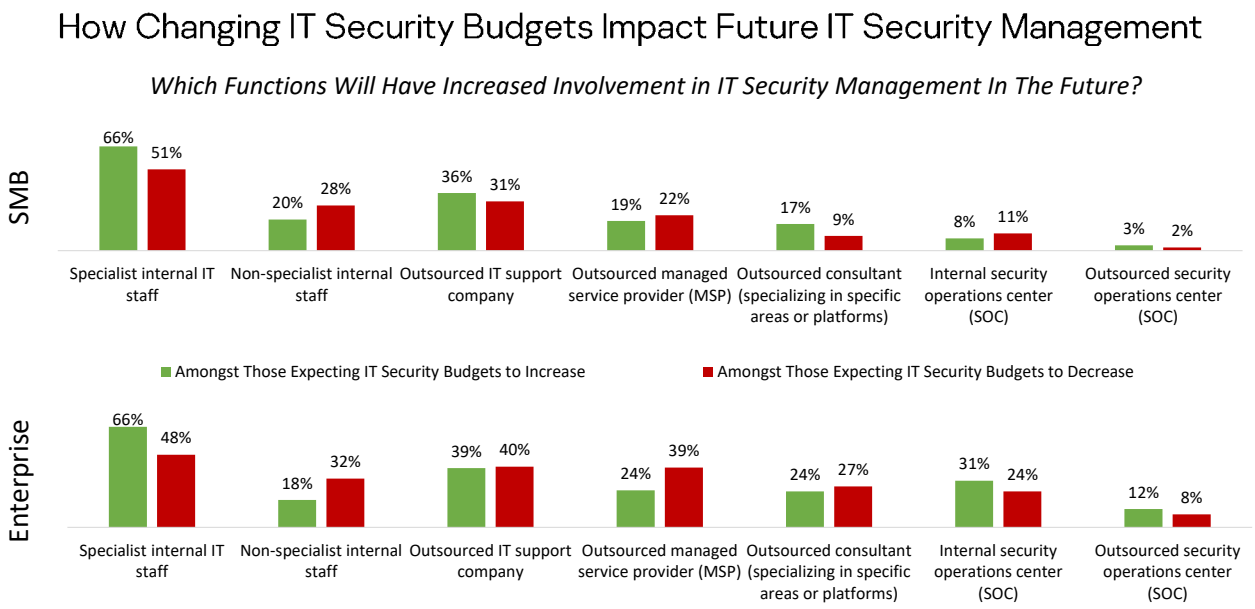

Figure 3. How changing IT security budgets impact future IT security management

It is evident that making the most of available budgets and ensuring the right resources and safeguards are in place is driving MSP business growth. But the same motivators can also be a deterrent for many potential businesses and industries to invest in external support.

The European MSP landscape: priorities and challenges

A 'typical' MSP

We have already established that the role and responsibilities of the MSP are changing, so it makes sense to reset where most MSPs sit in today's landscape in order to assess the specific opportunities and challenges they face.

The majority (57%) of MSPs we spoke to have between two and 20 employees and despite being small businesses, a third (32%) of them service clients with over 300 employees. 50% of MSPs work with a diverse range of customers across a variety of industries, with a third (35%) p rimarily focussing on supporting SMBs.

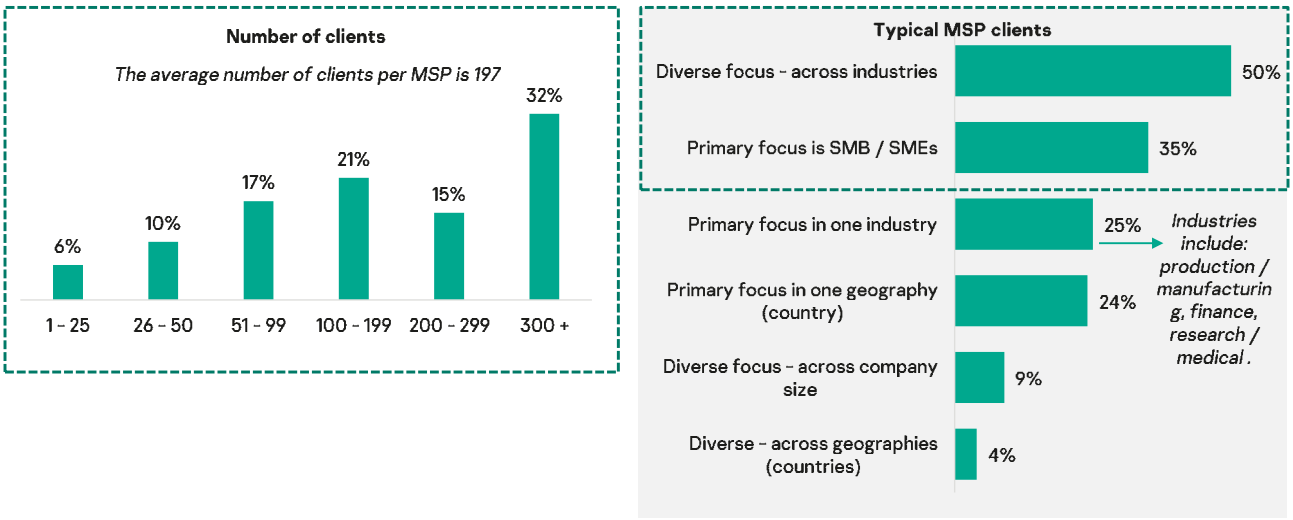

Figure 4. Number of MSP clients and typical MSP clients

With such a broad customer base, this can be a challenge for MSPs, who need to prove they understand and can support industry nuances and specific business pain points. As such, MSPs need to offer a wide range of services to clients to help meet their needs, meaning they must have proficient skills and expertise in a variety of areas.

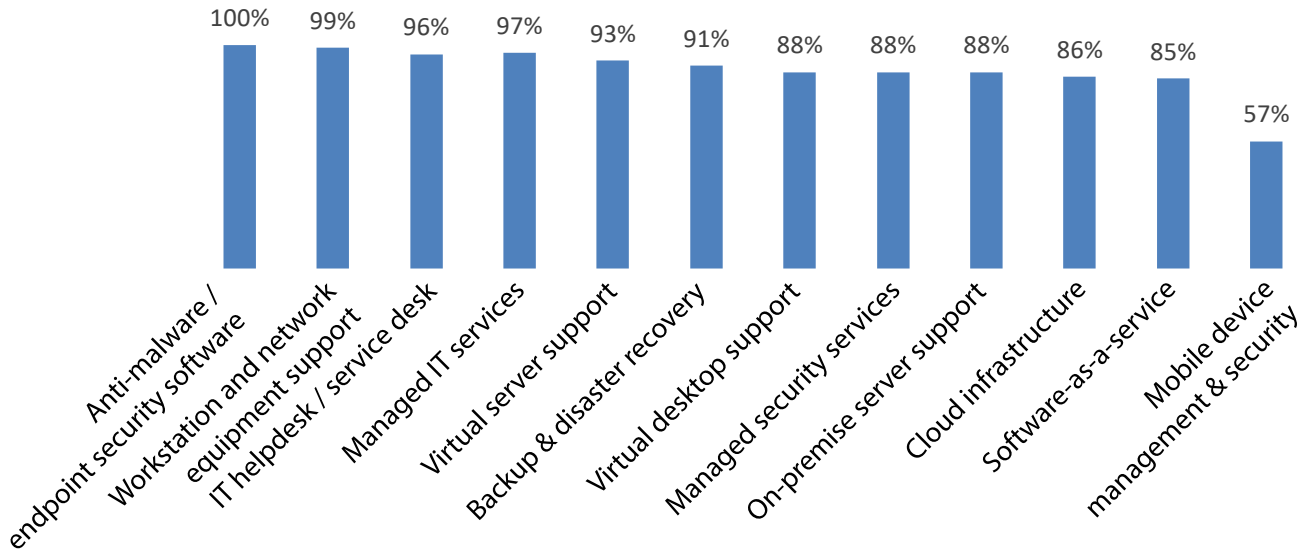

Figure 5. Overview of the main 'managed services' offered to clients

However, despite high client numbers, when it comes to the specific number of devices that MSPs typically manage, a quarter (23%) manage only between 10 and 25 per customer. For 48% of MSPs, this reduces to less than ten 'nodes' per client.

Pleasure and pain

A growing customer base can be a double-edged sword for MSPs. Despite businesses crying out for their services, this is increasing competition within the market making customers more demanding of their MSP than ever before. This is true for three quarters (75%) of MSPs who admit that demanding clients and users is a key challenge. The same number (78%) also consider it a struggle to find new customers, with two-thirds (68%) grappling to maintain profitability.

The issue of revenue is evidenced in the breadth of services that MSPs need to provide and the low levels of nodes they are actually managing per client. To help bolster their value for clients and provide increased revenue opportunity, MSPs could offer a discounted deal on security software to make the outsourced model more cost efficient for their customers and to lock them in for the long-term.

With customer satisfaction at the forefront of many MSPs minds, it is no surprise that retention figures are the main measure of success for 43% of MSPs, with 41% relying on client satisfaction surveys to assess how well their business is performing. On the flip side, measurements based on the value that MSPs are providing customers in terms of profitability (33%) and efficiency (20%) are lower.

When it comes to strategies for attracting clients, the majority (83%) of MSPs rely on word of mouth or recommendation to boost their customer base, making reputation management a key asset in the MSPs acquisition arsenal.

Despite these challenges, MSPs across Europe predict significant business growth over the next two years, with 63% expecting strong (up to 20%) revenue growth. This certainly reflects the current trend in the global market and supports the predicted annual growth rate of 9.3%.

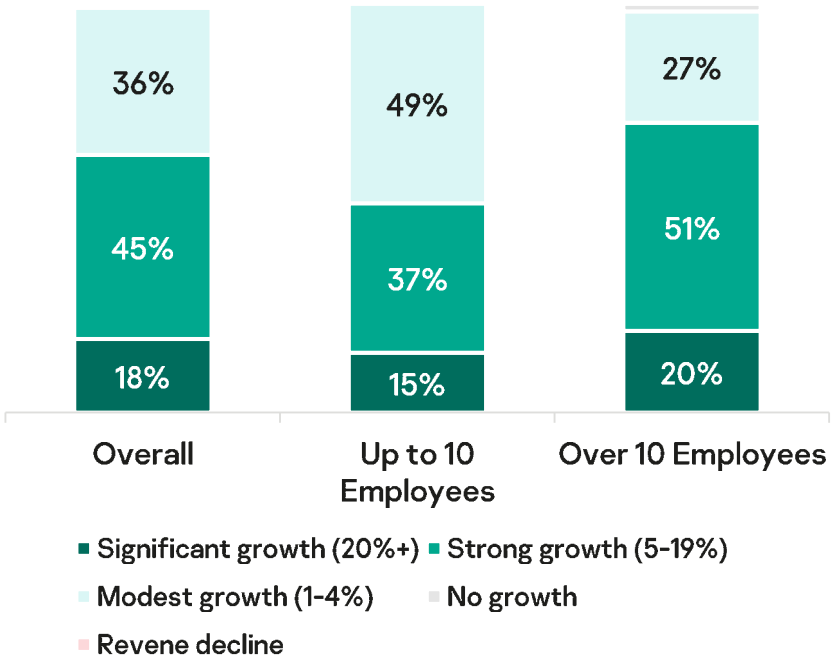

Figure 6. Expected MSP business growth

The perfect security partner

It is clear that outsourcing IT security management is high on the business agenda, so how can MSPs continue to fulfil this need and ensure the solutions and services they provide are up to the job. When looking to partner with an IT security vendor, 92% of managed services providers make the choice based on reputation and price. This is closely followed by ease of management, integration and license purchasing (88%).

The way that MSPs purchase licenses also has a bearing on risk and reward, helping to accelerate and simplify the delivery of services to customers. MSPs prefer flexibility in their licensing, with almost half (47%) stating they prefer to purchase individual licenses for each customer. Meanwhile, others (44%) chose to pay for IT security software and services from vendors through a monthly subscription model. Both of these options allow MSPs to protect themselves should a customer go elsewhere, but they can also manage their licenses more efficiently.

MSPs also prefer to use simple license ordering and management, and this is quite influential in their decision when choosing a security solution and vendor. In fact, more than half (56%) said that they use a vendor license management portal to obtain licenses. MSPs also benefit from remote monitoring and management (RMM), and professional service automation (PSA) tools integrated with security software for centralized monitoring and management, as well as automation of day-to-day routine tasks.

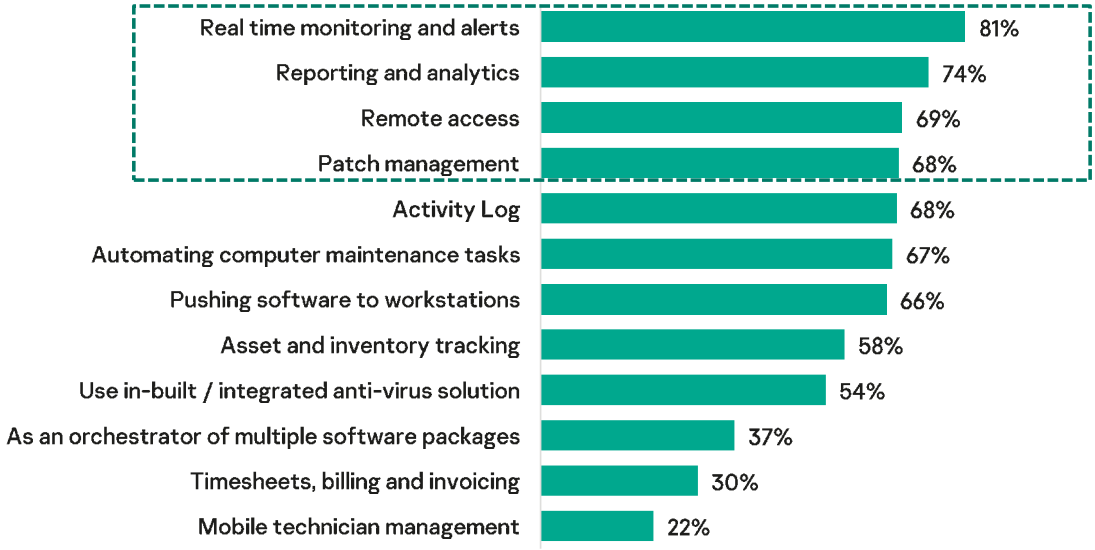

Figure 7. Main uses of RMM platforms among MSPs

Relationship highs and lows

Qualities versus challenges

As with any type of relationship, both parties expect to get a lot out of it but there are inevitably challenges and hurdles to overcome along the way. When it comes to expectations of today's MSPs, being an expert is the quality that clients look for above all others (84%), whether that's for on-premise or cloud infrastructure solutions. MSPs must also be able to help with compliance and regulations (82%), and respond quickly as well as adhere to high SLAs (80%).

Interestingly, cybersecurity capabilities in particular were highlighted as a key attribute that MSPs need to possess, by almost three quarters (74%) of clients looking for IT management support. The fact that this requirement features so high in the list of requirements is evidence that the ability to keep up with the evolving cybersecurity landscape is something that businesses need additional support with.

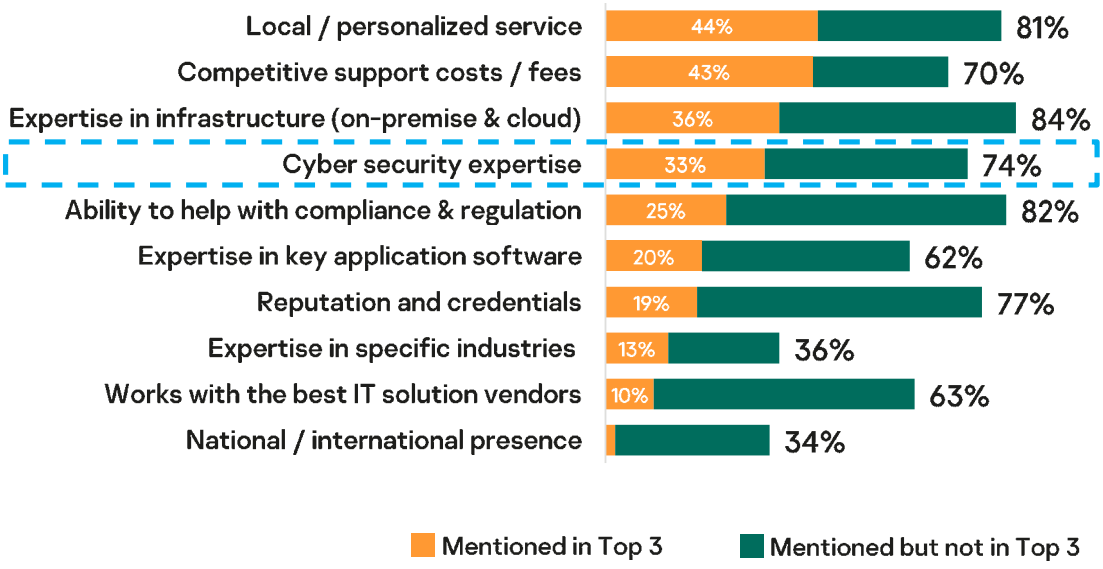

Figure 8. Qualities clients are requiring more from MSPs

In addition to these stated requirements, MSPs are also expected to deal with the unexpected. Unfortunately, being a trusted and expert provider brings additional challenges. Three quarters (78%) of clients expect MSPs to deal with issues outside of their contract. For others, it is the problems that users create that makes more work for them (65%) or an inability to follow helpdesk processes (59%) t hat adds unnecessary tasks to the 'to do' list.

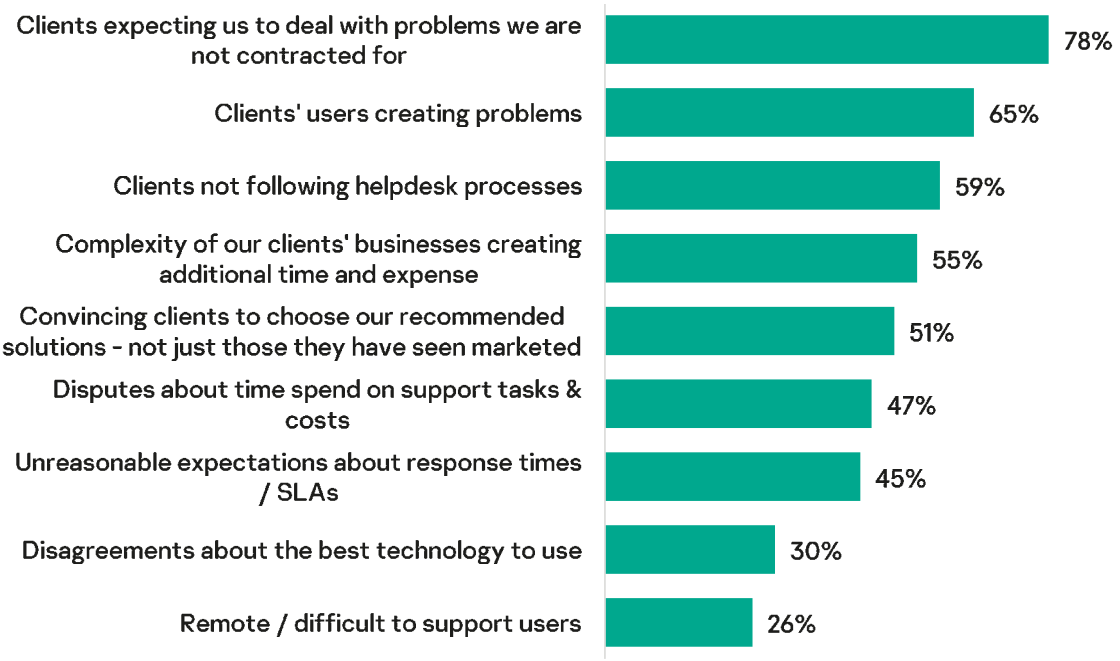

Figure 9. Pain points MSPs encounter with their clients

However, the biggest challenge facing MSPs is undoubtedly the volume of cyberattacks and malware infections leading to downtime for their clients (72%), closely followed by ransomware attacks (65%). But it's not just external threats causing a headache for MSPs, the human factor still leads to issues, with 69% of MSPs seeing user error and not following security policies as key threats to client security.

What this means for MSPs

The impact of any security incident can have far reaching consequences for not only the client, but the MSP involved. The recent Capital One data breach, which affected over 100 million individuals, was due to a 'misconfigured web application firewall on Amazon Web Services'. But although AWS was in the spotlight, it was not hacked, and the issue was put down to a customer who had failed to properly configure the cloud firewall.

This is just one example of where a third party can be in the firing line for a client data breach – and it certainly won't be the last. In fact, of the surveyed MSP clients that have suffered a data breach, 43% blamed their MSP, compared to only 41% who accepted that their own staff were at fault. What is more surprising is that a quarter (27%) of those who experienced a breach put it down to a lack of IT security knowledge by their service provider.

However, client security errors can also impact the MSP in terms of the time spent resolving the issue (67% agree), with a third (38%) even having lost money sorting out the problem which was not down to their negligence or lack of expertise.

Conclusion and recommendations

It is clear that reducing costs and making the most of available IT budgets is the main driver for companies to outsource their IT management. Coupled with a lack of internal resources and skills in IT security, there is a clear opportunity for MSPs to become cybersecurity experts and fill the security management gap for businesses across Europe.

It is therefore vital that MSPs are fully equipped to offer this level of service and meet the growing demand for outsourced security services. To help attract new customers and increase revenues, they need to expand the list of services they offer and focus on their market positioning and reputation management to come out on top over their competitors.

Customers expect security protection, but also expertise in information security from their MSP. Lack of competence in the field can lead to losing customers and failing to become the trusted advisor and partner that they crave. It is imperative for MSPs to build trust and loyalty with customers which can only be done by having the right tools and skills in place to support clients at every step of the way.

Reputation is key and just one slip up can have long lasting effects for attracting and retaining customers. Having the full breadth of security services, backed up by a strong and reliable cybersecurity partner will stand MSPs in good stead to realize the predicted market growth, driving profits and long-term business stability.

Vendors have a big part to play and can offer vital support to MPSs. It is no secret that MSPs are looking to expand their security services in the next few years, so vendors that can offer security assessments, incident response and email or web gateways look set to benefit from rising demands.

Security vendors can pass on important cybersecurity expertise and boost skills, as well as support with marketing and sales. The Kaspersky Managed Service Provider Partnership offers cybersecurity products dedicated for use by MSPs, together with specific cybersecurity training, education materials and events. Kaspersky has a broad portfolio designed for MSPs, allowing them to deploy either on-premise or cloud-based solutions – from endpoint protection through to hybrid cloud security, email and web access protection. These solutions can be integrated with remote monitoring and management (RMM) and professional services automation (PSA) platforms, to help service providers automate routine tasks. The partner program also includes marketing and financial benefits for all Kaspersky partners.

More information about the Kaspersky Managed Service Provider Partnership Program is available on the Kaspersky website.