

Got something to say?

If you have any comments to make on this issue, please e-mail: tom.paye@itp.com

Alain Penel

Attitudes to outsourcing



“Putting your enterprise IT security into a service provider’s hands, especially increasingly complex functions, requires a high level of trust and assurance.”

Alain Penel, regional vice president for the Middle East, Fortinet



As the job of securing business from cyber-attacks gets tougher and data privacy demands increase, new research commissioned by Fortinet shows that, far from going into in-house lockdown, IT leaders are increasingly considering managed security services.

In our latest global survey of over 1,600 IT leaders in large enterprises, decision makers revealed a growing appetite for managed security services, with a quarter citing ‘outsourcing some or all IT security functions’ to a managed security service provider as the single most important initiative for confronting the rising complexity and volume of cyber-threats in their organisations.

Over three-quarters of decision makers said functions like firewall, IPS and email protection would be suitable to apply to an outsourcing strategy in their organisation. However, these basic security functions, long considered for putting into a trusted service provider’s hands, are now being joined by functionality such as authentication, ATP sandbox and even DDoS mitigation. Today, only a minority of ITDMs believe that even the most advanced IT security

functions are unsuitable for outsourcing to a managed security service provider (MSSP). So, what’s changed?

Nine out of ten of the CIOs we surveyed said that the increasing frequency and complexity of threats is making the job of securing the business noticeably harder than it was just 12 months ago. And as high profile IT security attacks and national security scandals have become a common feature in news reports worldwide, this has seen a dramatic increase in pressure, awareness and involvement in IT security matters coming from the direction of the boardroom.

According to the IT leaders we polled, this serious boardroom pressure to keep the enterprise secure has jumped almost one-third in the last 12 months, making security paramount and a more pressing consideration over other business initiatives.

Add in demands for securely enabling employee mobility, and emerging technology like big data, and there’s a lot of weight on the shoulders of senior IT professionals today — causing them to re-evaluate their goals to ensure they strike the right balance to achieve resilience in the face of rising cyber-threats.

Ninety per cent of IT leaders, for example, stated they have been provoked into looking at new IT security investment and to re-assess their security strategy, due to rising data privacy concerns and securing big data initiatives.

It should come as no surprise, then, that the influencing factors for moving to managed security services are not led by cost and resource considerations, but by the need for always-on, high-performance, comprehensive, security infrastructure.

It was the increased complexity and scale of managing cyber threats that measured the largest driver to outsource, with half of all respondents selecting this as a key factor. This was closely followed by rising data

privacy challenges, whilst better financial models for procuring security followed in third and a lack of sufficiently skilled internal resources in fourth.

Whilst the benefits of outsourcing IT infrastructure and applications have long been understood, migrating to managed IT security services has often been held back due to concerns over 'letting go', especially amongst larger enterprises. However, as our IT leaders face the day-to-day reality of combating a relentless battle against the increasing frequency and complexity of threats, their attitude is changing.

When we asked about their own personal online security habits, 56% said they would be willing to trust their own personal data with a service provider that outsourced IT security. Along with this rise in as-a-service consumption in our personal lives, perhaps IT leaders are also emboldened by the increased acceptance and successful adoption of cloud services, as they are now recognising that, with the right due-diligence and sourcing strategy, IT security is also suited to this model.

Of course, putting your enterprise IT security into a service provider's hands, especially increasingly complex functions, requires a high level of trust and assurance. For the IT decision makers polled, it is reputation in the enterprise



↑ Businesses of all sizes are considering outsourcing their security operations, according to Penel.

market that wins out as the most critical attribute needed by an MSSP when winning their business.

Reputation was called out above portfolio of services offered, global scale of the organisation in third, and reliance on the SLA in fourth place as critical considerations when looking at a potential provider.

As the threat landscape has continued to evolve over the past 12 months, it is no surprise that businesses of all sizes are increasingly considering the managed security services model for cost-effective, multi-threat security solutions, and, perhaps most importantly, around-the-clock risk mitigation.

A demand fueled by compliance, greater executive awareness of IT risk and advanced persistent threats, combined with the need for sourcing expert security personnel and global threat-response intelligence — outsourcing security capabilities to managed security service providers is emerging as a key strategy for enterprises today.

With the majority of IT decision makers in our global survey citing high levels of rising pressure, and their job of protecting the business getting tougher, the rise of managed security services will indeed be an interesting trend to track, with all indications pointing to its upward trajectory. ●

“The rise of managed security services will indeed be an interesting trend to track, with all indications pointing to its upward trajectory.”