Executive Brief

Managed Security: Towards Chaos or Clarity?

Sponsored by: SecureData

Duncan Brown
November 2016

SUMMARY AND IDC OPINION

Three "mega" drivers are combining to create a fundamental transformation in the security industry. A dynamic threat landscape, business-led digital transformation and regulatory upheaval are collectively causing substantial consequences to the security operations of most enterprises.

Chief among these consequences is a resultant shortage in security skills and expertise, but they also include a greater demand for automation of security processes and a tighter integration between products in the typical security estate. The trouble is, most organisations lack the time, wherewithal or inclination to effect these changes.

This leads many organisations to conclude that managed security services (MSS) is a viable and attractive option to consider in delivering at least some part of their security operations.

MSS offers a variety of benefits to enterprises. Most immediately, it addresses the skills scarcity that all enterprises experience. There is also the opportunity to optimise security operations, and to benefit from the scale that MSS providers (MSSPs) offer. Many organisations also look to outsource commoditised activities that are essential yet relatively low in business value. MSS provides a degree of predictability of budget spend, as opposed to more ad hoc project-based use of external resources. Importantly, cost is not a common driver for the adoption of MSS.

MSS is not a trivial undertaking. Organisations do not take outsourcing of security lightly: in fact, their natural inclination is to keep operations in-house. Yet the compelling transformative forces affecting the industry compel enterprises at least to investigate MSS.

CISOs worry specifically about the loss of visibility and control in outsourcing security. MSSPs that are sensitive to these concerns and are able to create a high degree of trust and transparency can become valuable partners in the provision of state-of-the-art security operations.

OVERVIEW OF THE SECURITY MARKET

The security industry is undergoing a fundamental transformation in its focus, scale and agility in order to cope with seismic shifts in the demands from business and regulators. There are three "mega" trends that are driving the security market:

- The dynamic threat landscape
- Digital transformation
- Regulatory upheaval

The Dynamic Threat Landscape

Everyone involved in security of information systems is familiar with the growing threat of attacks. There are more attacks and successful breaches occurring more often to more organisations. All metrics for attacks and breaches are heading in the wrong direction. Irrespective of whether one

measures the absolute number of new attack types and variants, actual breaches, the cost per breach or the reputational damage caused, the data indicates that the situation is worsening on a daily basis.

Importantly, it's not just that there are more "bad things" happening: it is also the case that the threats and attacks are changing continually. This means that it is extraordinarily difficult to keep up with the attackers. Most security operations – and many security solutions vendors – are being out-innovated by threat actors.

This dynamic landscape of threats causes huge pressure on security operations teams, in terms of staff resources and skills, available countermeasures (including new tools and techniques), and budgets. CISOs need to get ahead of the threat actors, but they are barely managing to keep up.

There are somewhere between 500,000 and 1 million new malware variants produced each day (source: *Symantec Internet Security Threat Report 2016*, *Kaspersky IT Threat Evolution in Q1 2016*, *FireEye Annual Cyber Threat Report M-Trends 2016*), which require a new signature to be created and distributed to all end points. The latest sophisticated advanced threats apply techniques previously seen only in attacks from nation state actors, but which are now being used by criminal enterprises. Incidence of ransomware infections have increased by 300% since 2015.

The comforting thing about the dynamic threat landscape is that security professionals understand it. Threats may be increasing and changing but they are in the domain of the experienced CISO and security analyst. It is therefore arguable that organisations might be able to struggle on as they are, if the only concern was in the remit of traditional security operations.

But the increasing demands on security operations are not just coming from the attackers.

Digital Transformation

Keeping an organisation secure while dealing with a dynamic threat landscape is hard. But it is compounded if the business itself is changing in ways that challenges traditional security models. The biggest agenda item for CIOs – and many CEOs – in Europe is digital transformation, the shift to using 3rd Platform technologies in support of doing new business in different ways. Digital transformation is important because it changes the organisations' modes of interaction with their customers, their suppliers and partners, and their employees. Using the four 3rd Platform pillar technologies of cloud, social, mobile and Big Data/analytics, organisations can integrate with external parties in innovative ways, collaborate on document and idea creation, and engage on highly interactive platforms. Digital transformation changes organisations' ability to operate with the speed, agility and responsiveness required in today's business environment.

The rapid adoption of 3rd Platform technologies caught many security operations by surprise. The initial reaction of most was to block the use of cloud and mobile technologies, including bring-your-own-device. These technologies in particular represent a breakdown in an organisation's perimeter, the central security protective barrier that separates the good from the bad (or at least the unknown). Cloud and mobile technologies evaporate that perimeter, exposing the organisation to the known threats that the perimeter used to protect against, and a host of new ones as well. The security operations teams in most organisations react predictably: they try to stop technology adoption.

The key dimension of digital transformation is that it is a business-led initiative. IT professionals tend to hear "digital transformation" and focus on the "digital" part – the technology. But it is the transformation that is important to business, and business needs to drive the digital transformation projects forward. Digital transformation happens whether or not security wants it.

This often leads to organisations rolling out digital transformation programmes without the knowledge or buy-in of the security team. This might be because the security regime tries to disallow the use of the required technology, or the security team is disengaged from business, or security doesn't know

how to secure cloud, or a host of other reasons. Whatever, the business shifts to a mode of operation that is inherently insecure.

Securing digital transformation is tough. Perimeter controls are ineffective, and so new approaches and tools are required. These innovations are often unproven or at least unfamiliar, and their introduction places new constraints on a security operations team already stretched by the dynamic threat landscape.

Organisations therefore need to decide when to use digital transformation approaches, and how – or whether – to apply security controls, according to the perceived business risk. But that business risk is about to increase substantially.

Regulatory Upheaval

To date, most security operations have had no obligation to adhere to specific standards. Companies choose whether to accredit their operations to third-party certifications such as ISO 27001. Industry bodies sometimes implement regulations surrounding specific business processes: PCI-DSS for card payments is an example. Personal data regulations do exist, but these are fragmented and lightweight in most jurisdictions.

That is about to change.

The General Data Protection Regulation (GDPR) represents the biggest shakeup to data protection legislation in 30 years, and its implications on security (and several other technology categories) will be profound. It comes into effect in May 2018.

It is difficult to overstate the impact of GDPR. The increase to business risk is such that it is comparable with anti-money-laundering and anti-bribery legislation. The financial penalties are severe: a maximum of 4% of overall annual revenue or €20 million, whichever is the higher. The introduction of mandatory breach notifications will have an impact on reputational risk. And the ultimate sanction of a suspension of personal data processing (which would include payroll processing and taking orders from customers) should get the attention of any board, however sceptical of the importance of GDPR.

GDPR is almost cursory in its consideration of security, other than to say that it is a fundamental principle. Article 5 mandates that data must be "processed in a manner that ensures appropriate security of the personal data …". Article 25 mandates data protection "by design and by default", which means (in effect) that data protection – and by extension, security – must be considered at the very conception of an idea to process personal data. Article 32 (security of processing) suggests some technology approaches, such as encryption, business continuity and testing, but is otherwise non-specific about security techniques. However, Article 83, which lays out the consequences for getting data protection wrong, leaves no doubt as to the importance of security. Security measures, or lack thereof, will determine an assessment of "the degree of responsibility of the controller or processor", which is a mitigating factor in the imposition of administrative fines.

What does this all mean? It means that organisations must take a detailed and considered view of what security capability to operate in their organisations, after a rigorous assessment of business risk. Given that business risk increases with GDPR, it is extremely likely that most organisations will require at least some security capability to be upgraded.

The impact here is significant, since security operations are already busy dealing with the dynamic threat landscape and the demands of digital transformation. Regulation compounds the pressures already on organisations' security capabilities.

What Does This Mean for Security Operations?

Dealing with any one of the three "mega" drivers puts unprecedented pressure on any enterprise's security operations. But the combination of all three drivers means that security operations now need to change the things that they do and the way in which they are done.

There are several consequences of these three converging megatrends. The first is a dearth in available security skills. The security skills shortage is a global concern, and it is a direct consequence of the rapid increase in demand on security operations teams and the increased risk to business.

The second consequence is a desire for greater automation and integration of products in the typical security estate. The dynamic threat landscape has resulted in enterprises buying point solutions to address specific threats, but this has resulted in a highly complex and diverse security estate of individual tools. The management overhead is substantial, and so CISOs are looking for solutions that reduce the intervention of staff.

The third consequence is a drive towards simplification of security estates. This means a shift away from best-of-breed solutions, towards a more integrated set of technologies. This can either be achieved by selecting more products from fewer vendors (assuming that those vendors' products integrate well together) or a bespoke integration exercise.

The problem for most enterprises is that they don't have the time, resources, skills or budget to implement fundamental changes to their security operations. Many are therefore evaluating the consequences of the three "mega" drivers and concluding that some (or in some cases all) of their security operations should be outsourced to a managed security services provider.

THE ROLE OF MSS IN MODERN SECURITY OPERATIONS

Managed security services is the fastest-growing segment in the already buoyant security market. It is growing faster (12.4% CAGR 2015–2020) than any of the product-based segments (averaging 5.7%). What is driving this growth?

MSS Addresses the Skills Scarcity

The primary driver for the adoption of MSS is to address the lack of available skills. Many organisations position security as an essential but commoditised business operation. It requires specialists, but these are difficult to recruit and retain. Enterprises that do not differentiate their businesses on security find the prospect of MSS attractive. MSSPs have both the in-house expertise and scale to deliver security outcomes that meet or exceed normal business requirements.

Optimising the Security Operation

Many organisations capitalise on their MSSPs' capabilities and seek to optimise their existing security operations. This may be facilitated by a reduction in the number of tools in the enterprise security estate, better integration between those tools, or through the application of better security business processes.

Benefitting from MSS Scale

The scale at which MSS providers operate is beyond all but the largest enterprises. Security operations work best at scale, benefitting from a broad set of events and intelligence across a large set of enterprises. Most enterprises do not experience the number and variety of events sufficient to justify the expense of a dedicated security operations team. Enterprises also struggle to fulfil the career aspirations of in-house security analysts, who may be tempted by more varied work elsewhere.

Outsourcing Commoditised Activities

MSS creates an opportunity for enterprise to externalise low-value activities through industrial-scale delivery models. Providers can remove the responsibility for repeatable but lower value elements of security operations, such as security event monitoring and appliance management. MSSPs have the advantage of scale and industrialisation, and are typically most advanced in the adoption of security automation technology. This allows them to offer services at lower cost while arguably also increasing the quality of outcomes. Enterprises like this approach because it allows their scarce internal resources to focus on the most critical activities.

Budget Predictability

Almost all enterprises use external resources for at least some of their security activities. This may be for ad hoc projects, but this impacts their discretionary security budgets. MSS, on the other hand, presents an opportunity to procure security services at a more predictable expenditure rate. The ability to work with MSSPs on a per-event or managed device basis, or even tied to specific security outcomes over a fixed period of time, can be attractive for enterprises.

Cost is a Consideration, Not a Driver

Importantly, cost is rarely a factor in deciding whether or not to outsource security to an MSSP. Although budgetary considerations come into play in the selection of a vendor, they do not often drive the initial decision to outsource. This is because security remains a vital part of an enterprise's responsibilities and so the decision to outsource is always based on a strong business rationale rather than purely financial measures.

MSS CHALLENGES

No enterprise outsources any aspect of its security without being diligent in the construction of its rationale and business case. Security is too important to leave to chance. In addition, most CISOs have a cautious and conservative mindset that determines their instinct towards security. Their starting point is always to keep security in-house.

This is because security professionals need to understand the security posture of their organisation at any given moment. This mandates a high degree of visibility of their security estate and the events that are being recorded against it. When something happens, CISOs want to know about it quickly.

CISOs also worry about control of their environment. The setting and maintenance of policies is a critical part of their responsibility, and they need to ensure – for compliance or business process reasons – that agreed policies are being adhered to.

These twin concerns of visibility and control act as inhibitors for the adoption of MSS. However, enterprises need to be careful not to confuse the need for visibility and control with the exclusively in-house operation of security functions. It is perfectly possible to retain both visibility and control of security operations while outsourcing these to a third-party provider, when done correctly.

MSS does require careful assessment of potential providers as CISOs seek to reassure themselves that levels of visibility and control are maintained, if not enhanced. This reassurance hints at the key attribute of the relationship between an enterprise and its MSSP: trust. A mutual understanding between the customer and provider is fundamental to a successful partnership.

Trust can be established in several ways. It can be brokered by an independent third party, such as a reference customer. CISOs are cautious by nature and rarely want to be the early adopter of security innovations. The comfort of hearing from a peer enterprise that has successfully outsourced security operations significantly de-risks their own venture into MSS.

Trust can also be created through small projects that establish a good working relationship and evince the required level of expertise. Systems implementation is an obvious segue into MSS, but smaller engagements such as pen testing and security audits can also establish confidence.

In all cases, transparency of operations is vital. It is imperative that the MSSP not only operates the security activities effectively and efficiently, but is also able to demonstrate this. This is important not only to the CISOs themselves, who wish to be assured that all is well, but also to other stakeholders such as senior management, who these days have a close interest in security.

RECOMMENDATIONS

One MSS Size Does Not Fit All

There is a common perception that MSS is only for large and mature security operations. In fact, one of the fastest-growing areas of adoption of MSS is in the midsize enterprise sector, and this is driven largely by the adoption of cloud-based MSS.

Indeed, IDC tracks three variants of MSS: on-premise, hosted and cloud-delivered. On-premise MSS is by far the largest segment, but cloud and hosted (private cloud) MSS is an attractive option for those organisations comfortable with off-premise architectures.

Many organisations remain concerned at the security of the cloud, but the cloud is not a uniform environment. It is perfectly possible, and increasingly common, for cloud environments to be at least if not more secure than is possible in on-premise implementations at comparable cost.

IDC therefore recommends that enterprises investigate MSS offers in both on- and off-premise configurations.

Key MSS Attributes

In choosing a provider of MSS there are a number of primary considerations. The first of these is expertise. A core premise of MSS is the availability of otherwise scarce resources at affordable prices. Therefore, the capabilities and qualifications of individual staff are an important aspect of MSS providers.

Also important is the scale of operation. It is not necessary to be the very biggest MSSP but it is important to have sufficient size to deliver the benefits of scale to customers. However, it is also necessary to be able to focus on the individual needs of each customer, and this requires a degree of intimacy and understanding. Getting this balance right between scale and individualisation can be a tricky manoeuvre.

Finally, it is important to present MSS as transparently as possible. CISOs detest a black box approach to MSS as it obfuscates the visibility and control that they crave.

Start Small and Grow Steadily

Few enterprises engage in wholesale outsourcing of security operations in the first instance. There is usually a (sometimes prolonged) period where certain low-risk security operations are outsourced as a first step. This is characteristic of the vast majority of MSS adoption: CISOs engage with MSSPs cautiously and selectively. Trust is built over time and, assuming a successful initial period of operation, then leads to a greater shift in operations to the provider.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC U.K.

IDC UK
5th Floor, Ealing Cross
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Copyright and Restrictions