Operators must partner with mature MSSPs if they are to succeed in enterprise security services

January 2018

Patrick Donegan

A few of the world's largest telecoms operators – such as AT&T, BT, Singtel, Telstra and Verizon – are already significant players in the global managed security service provider (MSSP) market servicing large enterprises. However, most telecoms operators do not have a significant role in this market – they won just 17% of the USD12 billion of addressable spend by large enterprises on security in 2016.

We expect demand for managed to security to grow. Cyber-security threats are likely to continue to escalate, and many enterprises want to outsource at least some of their security requirements. Telecoms operators that are not currently MSSPs are looking at how to enter this market. This article is based on Analysys Mason's recently published report, *Cyber-security services for large enterprises: opportunities for operators*.

Most operators will need partners to enter the MSSP market

Most operators cannot expect to succeed as new-entrant MSSPs on their own. At its inception, the MSSP market provided basic managed firewall services on the customer's premises. Telecoms operators were – and still are – capable of delivering that themselves – on premises or in the cloud. However, the portfolio of services required to succeed as an MSSP – and the skillsets required to deliver them – has moved on.

To protect enterprises from the cyber-security threats of today, MSSPs need to offer a broad menu of security services, delivered from a security operations centre (SoC) that operates 24 hours a day, 365 days a year. Services include:

- managed vulnerability scanning
- distributed denial of service (DDoS) protection
- security information and event management (SIEM) monitoring
- protection against advanced persistent threats (APTs)
- event reporting and incident response
- proactive threat hunting.

MSSP must invest and have data analytics, machine learning and threat intelligence expertise if they are to compete in this market. They also need large teams of cyber-security analysts, which are in short supply and costly as a result. To give a sense of the scale required, established MSSPs SecureWorks and Trustwave have around 2400 and 1700 employees respectively. The cyber-security talent pool is hard to retain for all but the most competitive companies at the cutting edge of developments.

Most telecoms operators would find it challenging to build a new MSSP business

Rather than try to build an MSSP solution alone, the obvious solution for most telecoms operators is to become a channel partner for the large, established MSSP players. These include BAE Systems, IBM Security, Raytheon, SecureWorks and Symantec as well of some of the MSSP arms of operators previously mentioned.

These MSSPs are also seeking local partners, a role for which telecoms operators are well positioned. Many MSSPs are based in the USA and have relied on their domestic market and Fortune 500 companies. To achieve long-term revenue growth, they need to expand by serving large national corporates in other regions. Until now, these large national enterprises have been underserved by the biggest MSSPs, especially outside the USA. Telecoms operators, with their existing relationships with large enterprises, are well placed to support the ambitions of MSSPs.

Examples of partnerships between telecoms operators and MSSPs already exist.

- **Trustwave with Singtel and Rogers.** Trustwave is owned by Singtel and has partnered with Optus (Australia) and Singtel's affiliates, beginning with Globe in the Philippines. Trustwave also has a deal in place with Rogers (Canada).

- **BAE Systems and O2 UK.** The two parties collaborate to provide managed security services and cyber-technical services, either as a standalone service or in conjunction with O2's 'O2 Gateway' proposition.

- **IBM security and an unnamed Asia–Pacific operator.** IBM Security has one telecoms operator partner – in Asia–Pacific – but it is open to further partnerships.

SecureWorks' management has given guidance to investors that it is looking for new channel partners in Europe and Asia–Pacific. The company stated that it hoped to finalise on one or more of these deals before the end 2017.

Partnerships between MSSPs and operators will be difficult to manage

Established MSSPs and telecoms operators have potentially powerful synergies, but they should be aware of the scale of the challenge involved in executing the partnership. MSSPs manage and integrate multiple hardware and software components of their own as well as those from third-party vendors to deliver a reliable service in line with contractual commitments and service-level agreements (SLAs).

Delivering a competitive suite of managed security services predictably and consistently from within the complex MSSP ecosystem is challenging enough. Introducing a telecoms operator's IT and network environment – including its BSS/OSS environment – as an intermediary between the MSSP and the enterprise customer adds further complexity.

If this complexity across the MSSP and operator domains is not managed effectively, it risks jeopardising:

- service availability
- the ability to meet or commit to SLAs
- time to market
- the ability to bill for services.

Prospective partners must commit to a detailed process for anticipating, explaining, managing and tracking the impact of frequent changes in one another's environments. They must also understand and collaboratively manage the end-to-end impact of changes on the customer's experience of a managed security service.

Most telecoms operators that want to capture the revenue opportunity presented by cyber-security threats to the enterprise need to commit to partnerships with leading MSSPs. To make themselves compelling partners, each party needs to be able to understand and align with the other's digital transformation roadmap.