



Building managed services for security

A Canalys report for Kaspersky

Contents

Key findings	3
MSP and security market overview.....	4
Building a stronger MSP posture.....	9
Ten steps to a more secure practice.....	11
Key takeaways.....	18

Key findings for MSPs

1

The rising digitalization of customers' businesses is putting further pressure on the ongoing IT skills gap, which increases the need for outsourced IT services. That digitalization is also fueling the exponential growth in cyber-criminality, which in turn drives the need for more critical security managed services.

2

Developing an MSP "operating system" or posture is the key to maximizing profit in your model. Many partners deliver services in manual or ad-hoc ways, but even mature MSPs are always re-iterating their methods. Start by becoming your own MSSP, building better internal processes and using these to create a security services framework for customers.

3

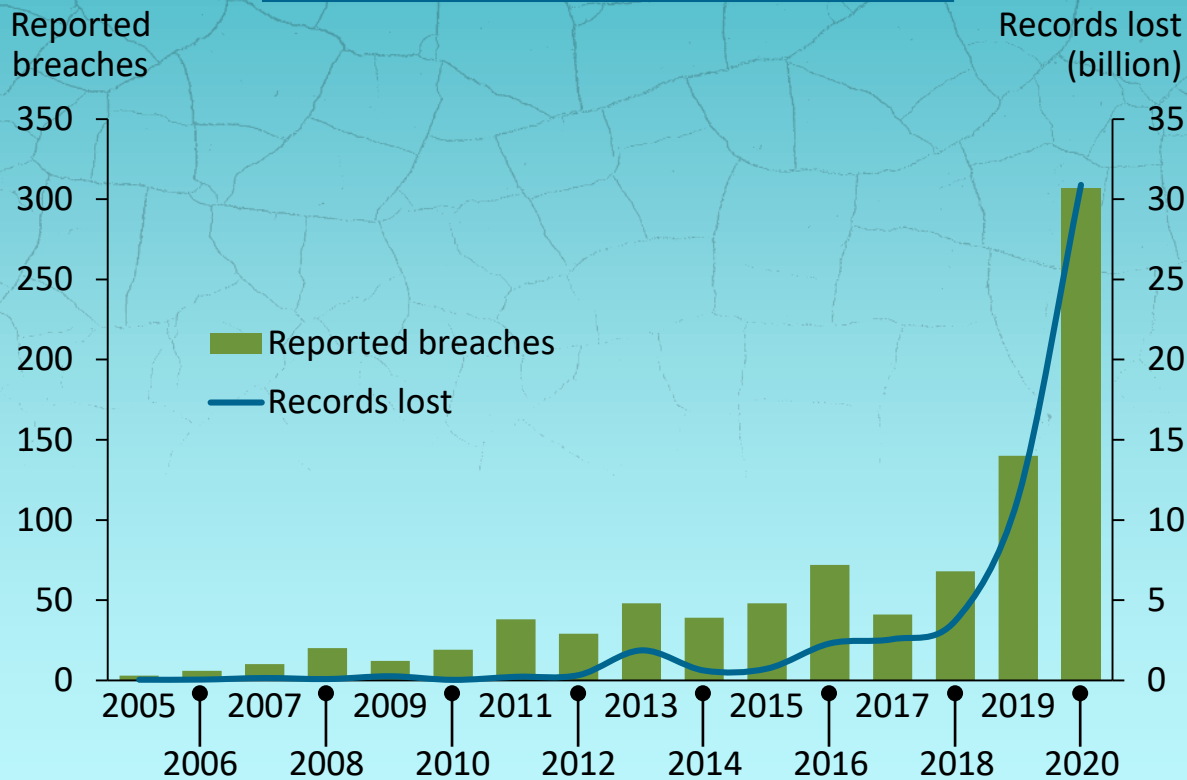
Breaking down the development of your MSP practice into steps can help you see the future more clearly – set goals for what you can do today, tomorrow and in the future.

“The difference between MSPs and MSSPs is contracting as partners and customers take a security-first approach to their digital deployments.”

Robin Ody, Senior Analyst, Canalys

Digitalization deepens the data breach crisis

Reported breaches and records lost



Since 2005, at least 55 billion **data records** have been compromised in 900 known **breaches**.

77% of these data records were compromised in the last two years alone, with 2020 being the worst year on record.

Over the last 12 months, 31 billion data records were known to have been compromised, up 171% from a year ago. This represents a major escalation of a crisis that had already deepened in 2019.

The main factors contributing to this rise include the failure to secure and encrypt Elasticsearch servers, as well as correctly configuring cloud-based databases.

The acceleration in digital transformation projects and continued remote working will maintain this trend in 2021.

MSPs around the world face similar challenges



MSPs will need to become their own MSSPs

As MSPs are increasingly the key attack vector for hackers, customer scrutiny will only grow. Following the rise in attacks on MSPs, over two thirds are reviewing the technology they have invested in and the security processes they engage in.

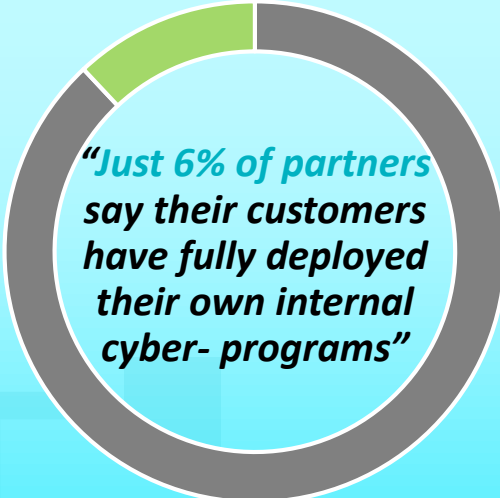
But nearly **75% of MSPs do not currently offer a security managed service**. The divergence between customer needs and partner business models will increase M&A as partners look to add skills; this will boost the value of cyber-skills in particular.

Building an MSSP practice can be complex, but improving your own cyber-posture is one of the strongest opportunities for developing auditing and deployment frameworks for your customers.



“The most valuable internal IT tools for MSPs are RMM, PSA, backup, networking tools and cloud productivity.”

Robin Ody, Senior Analyst, Canalys



“Just 6% of partners say their customers have fully deployed their own internal cyber- programs”

Ten steps to a more secure MSP practice

Process steps

- 1 Prioritize the security elements of your portfolio
- 2 Assume you are already under attack
- 3 Stay up to date with the latest patches
- 4 Proactive training for employees and customers
- 5 Audit all internal tools and service level agreements

Technology steps

- 6 Enforce MFA for all remote logins
- 7 Always use secure network and system infrastructure
- 8 Restrict admin access during remote logins
- 9 Create least privilege access for resources
- 10 Upgrade networking tools for hybrid working



Key takeaways

MSPs and cybersecurity

The gap between MSPs and MSSPs is getting smaller; any MSP that does not have a security-first posture is a risk for its customers.

Develop your MSP posture

Automating manual processes and providing standardized service delivery models can help to boost profitability and helps you to focus on revenue drivers, not ops.

Make your internal security as good as your external security

MSPs have become one of the key vectors for attacks; strong internal security can help build better solutions.

Invest in developer skills

Many partners are growing investments in software development skills, though this does not mean significant headcount needs to be added.



Insight. Innovation. Impact.

The written content of this document represents our interpretation and analysis of information generally available to the public or released by responsible individuals in the subject companies but is not guaranteed as to accuracy or completeness. It does not contain information provided to us in confidence by the industry. Market data contained in this document represents Canalys' best estimates based on the information available to it at the time of publication.

Canalys has a liberal policy with regard to the re-use of information that it provides to its clients, whether within reports, databases, presentations, emails or any other format. A client may circulate Canalys information to colleagues within his or her organization worldwide, including wholly-owned subsidiaries, but not to a third party. For the avoidance of doubt, sharing of information is not permitted with organizations that are associated with the client by a joint venture, investment or common shareholding. If you wish to share information with the press or use any information in a public forum then you must receive prior explicit written approval from Canalys.