Managed Security Services

Market Analysis
Abstract

April 2017
research.nelson-hall.com

Who Is This Report For?

NelsonHall's "Managed Security Services" report is a comprehensive market assessment report designed for:

- Sourcing managers investigating sourcing developments within the managed security outsourcing market
- Vendor marketing, sales and business managers developing strategies to target ITO service opportunities within managed security services
- Financial analysts and investors specializing in the IT services sector, including IT security services.

Scope of the Report

The report analyzes the worldwide market for managed security services and addresses the following questions:

- What is the market size and projected growth for the global managed security services market by geography?
- What is the profile of activity in the global managed security services market by industry sector?
- What are the top drivers for adoption of managed security services?
- What are the benefits currently achieved by users of managed security services?
- What factors are inhibiting user adoption of managed security services?
- What pricing mechanisms are typically used within managed security services and how is this changing?
- Who are the leading managed security services vendors globally and by geography?
- What combination of services is typically provided within managed security services contracts and what new services are being added?
- What is the current pattern of delivery location used for managed security services and how is this changing?
- Which services are delivered from onshore and which from offshore?
- What are the challenges and success factors within managed security services?

Key Findings & Highlights

NelsonHall's market analysis of the managed security services market consists of 54 pages. The report focuses on multi-year managed security services contracts, as opposed to those which are part of systems integration and short term projects.

Issues currently affecting cybersecurity can include:

- Cybersecurity has never before had such a widespread effect as it does now. The public consciousness has been besieged by news of cybersecurity affecting commercial organizations and also directly affecting the political environment
- While cybersecurity may be in the public consciousness, the average IT security literacy of the populous has not improved; organizations are still vulnerable from attacks such as phishing which target employees who are not aware how data should be shared
- Organizations now have more complex IT solutions through digital transformation, IoT, and the cloud; more data is collected, and the organization has less direct control over infrastructure and systems
- Cybersecurity talent is becoming increasingly difficult to hire, with organizations noting that skills shortages are directly affecting organizations' abilities to defend themselves. As the security landscape is constantly evolving, organizations need to perform their own (or subscribe to) advanced security research that is focused on both the wider security market and on targeted cybersecurity updates, e.g. industry-related attacks
- To increase the defenses of organizations, in the last few years there has been an increase in new regulations that organizations are required to meet. While these regulations can help organizations to keep their IT infrastructure and data secure, regulation has lagged behind the proliferation of newer IT solutions such as IoT.

Lessons that organizations for cybersecurity attacks include:

- The use of botnet based IT cybersecurity attacks can result in non-cybersecurity cost: vendors need to build cybersecurity response services with built-in detailed response plans that take into account how to communicate cybersecurity breaches to clients (to reduce reputational damage) and through partnerships, with insurers offering cyber insurance
- The motives for attack are varied: it is likely that every organization that holds some form of value is a target, whether this is for direct monetary gain using stolen IP, customer, or employee information; or for information that can be used to disrupt the operations of a competitor, e.g. nation states
- IT literacy does not equal cyber-literacy: cybersecurity training is required for employees who hold information or who could be used as a gateway to information for cyber-attackers, due to shared passwords
- Highly sensitive information is stored on systems: the volume of information on these systems is increasing. While personal information has been used directly or indirectly for monetary gain for years, the use of systems such as ubiquitous mobile technologies and IoT has given an unprecedented window into users' information, e.g. the use of voice assistants recording conversations. In addition, the sensitivity of the data has increased as biometric data is used

- Infrastructure at risk: while organizations may strive to secure their infrastructure and data, large scale destructive attacks can be used against the wider internet infrastructure, which does not have sufficient DDoS protection.

Contents

Report Length

54 pages, consisting of 8 chapters

Report Author

Mike Smart

mike.smart@nelson-hall.com

Vendors Researched

Atos, Capgemini, CGI, CSS Corp, HPE ES, IBM, Infosys, SecureWorks, TCS and Unisys