NelsonHall
Success through insight

Managed Security Services

Market Analysis
Abstract

August 2015
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?
- What 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 78 pages. The report focuses on multi-year managed security services contracts, rather than contracts which are part of systems integration or short term projects.

The profile of security attackers has changed, from lone attackers to organized crime and cyber espionage at a national level. The cause of the attacks have changed as the attacker profile changes, for example lone attackers a decade ago may have targeted a very high number of email addresses with a phishing scheme, for which the attacker would get a low response rate with each hit, providing a nominal reward. Organized cybercriminals, however, may now be performing attacks targeted at a specific organization over a long period, with the express purpose of copying the organization's IP, or silently disrupting the organization's operations, to gain a competitive advantage.

The general populace is more aware of cybersecurity through the reporting of insider threats such as Snowdon and Wikileaks or mega breaches. Coupled with an increasing number of government regulations on the storage and security of client data, it has become increasingly important for organizations to have an IT security strategy.

With the growth of third party storage such as cloud based storage, a number of organizations have moved from internally managed databases to third party solutions. This move typically causes a disconnect within the organization's security operations, and creates a more attractive target for attackers.

The increasing use of cybersecurity can be attributed to:

- Increasing cost of cybersecurity
- Access to cybersecurity skills and up to date information
- Ability to respond quickly to threats
- Ability to gain a holistic view of cybersecurity
- Strengthening social engineering around security
- Uneven workloads inherent in IT security.

IT security services can broadly be split between application and infrastructure security:

- Application security includes activities in support of the clients' applications or endpoints, with services including vulnerability testing/management, endpoint security management, application firewall, identity access management (IAM), and application secure development lifecycle (SDLC)
- Infrastructure security includes activities in support of the client's network, whether this is external or internal, and the information transferred across the network. Services include vulnerability management, SIEM, firewall management, network data loss prevention (DLP), intrusion detection/prevention services (IDS/IPS).

Contents

Report Length

78 pages, consisting of 7 chapters

Report Author

Mike Smart

mike.smart@nelson-hall.com

Vendors Researched

CGI, Cognizant, CSC, CSS Corp, Dell, Dimension Data, HP, Mindtree, Symantec, TCS, Unisys, Wipro