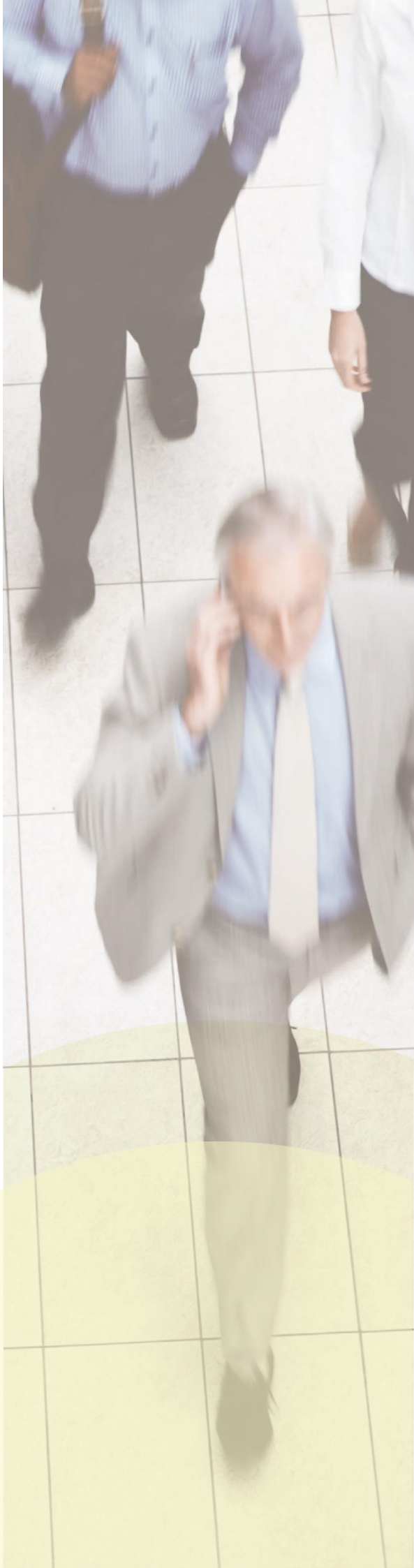
Managed Security Services

Market Analysis
Abstract



July 2018

www.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 50 pages. The report focuses on multi-year managed security services contracts, as opposed to as part of systems integration and short-term projects.

Issues currently affecting cybersecurity can include:

- Cyberattacks have become increasingly complex and easier to perform, state-built tools such as EternalBlue, and tools such as Autosploit allow an attacker to perform sophisticated attacks far easier than before
- With an increasing number of exploits that are discovered, vendors are releasing a large number of updates and patches
- Organizations have to consider how to set and monitor employees as the human factor in cybersecurity becomes increasingly important. This is especially important as IT security literacy remains fairly low with email phishing attacks remaining fairly common. These attacks are now more targeted at members of organizations that have the most access, i.e., exec-level, legal, F&A, and HR departments
- Year on year the public consciousness has been besieged by more news of cybersecurity not only affecting commercial organizations but also directly affecting the political environment, as such the amount of reparations demanded for infringements have increased and it is not uncommon for C-level exec's to resign after a large cyber attack
- Organizations now have more complex IT solutions through digital transformation, IoT, and the cloud; more data is collected, and organizations have 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 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:

- Recent cyberattacks demonstrate how org's should look to reduce vulnerabilities
- Best practice, e.g., patching or following cyber alerts, reduces the number of attacks
- Existing attack vectors are becoming easier to exploit, and new attack vectors are being discovered
- Attackers and defenders are focusing on the psychology of cyber attacks
- New technologies will drastically change how we manage cybersecurity.

Contents

Report Length

50 pages, consisting of 8 chapters

Report Author

Mike Smart

mike.smart@nelson-hall.com

Vendors Researched

Atos, Capgemini, DXC Technology, IBM, Infosys, SecureWorks, TCS, Unisys, and VirtualArmour