Cyber Resiliency Services

Market Analysis
Abstract

May 2019

www.research.nelson-hall.com

Who Is This Report For?

NelsonHall’s “Resiliency 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 Resiliency Services
- Financial analysts and investors specializing in the IT services sector, including Resiliency services.

Scope of the Report

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

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

- Organizations traditionally separating cybersecurity from business operations, with CISOs often struggling to present business cases and ROI of cybersecurity and build responses into BCM plans
- An increasing number of applicable regulations for organizations to meet, including those set from regions other than the organization's operations. These are too often seen as the standard level of defence, despite lagging behind new technologies such as IoT and blockchain
- Organizations having a large number of legacy applications that require investment to patch. Organizations may find this patching process uneconomical for the risk of being attacked
- Cybersecurity talent continues to be incredibly hard to hire, even more so for talent that have a business background and can relate the issues of cybersecurity to the organization's operations
- Increased sophistication of attacks with hackers using exploits developed by state-sponsored organizations that further their spread or make recognizing spoofing more difficult
- An increasing amount of data being collecting on customers which should they be breached can damage the organizations reputation
- The often overlooked human factor of cybersecurity for which users are unaware of what IoCs look like and how to react to an IoC.

Organizations can benefit from outsourcing cyber resiliency services through:

- Being able to leverage cybersecurity R&D and best practices from vendors with a much greater scale than they could achieve individually to give them a much better understanding of the threats that exist and are relevant to the organization and for the use of new technologies produced vendors such as AI for cybersecurity
- The ability to influence cyber insurance premiums through the use of risk analysis
- Using risk analyses performed by vendors to build ROI of deploying cybersecurity solutions and procedures
- The ability talk learn cybersecurity and spread awareness of cybersecurity through the organization from training programs which have been tried and tested across a large number of organizations
- The ability to leverage highly scalable, highly skilled teams when talent is too costly to hire, and leverage the highly skilled teams for the likes of legal consultancy
- Understanding how the organization can build cybersecurity into new products and services through DevSecOps and position cybersecurity as a differentiator.

Contents

Report Length

54 pages, consisting of 8 chapters

Report Author

Mike Smart

mike.smart@nelson-hall.com

Vendors Researched

Accenture, Atos, Capgemini, Deloitte, DXC Technology, EY, IBM, LTI, NTT Security, SecureWorks, Sopra Steria, and TCS