NelsonHall Market Analysis

Cyber Resiliency Services

Report Abstract

January 2021

By Michael Smart

Industry Sector Analyst

NelsonHall

47-pages

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 47 pages. The report focuses on cyber resiliency services contracts.

Issues currently affecting cybersecurity can include:

- An increasing number of regulations that carry the risk of fines
- Backups can be difficult to manage and are subject to regulations, for example, incorporating GDPR's right to be forgotten, and add data storage costs
- Cyber resiliency awareness is low within organizations and remains one of the major areas of vulnerability
- Difficulty in keeping abreast of evolving best practices for next generation technologies such as cloud, IoT, RPA, blockchain, and quantum
- Organizations holding a large number of legacy applications which require heavy investment to patch to meet required standards. Organizations may find that patching these applications is uneconomical
- Increasing ease and sophistication of attacks. Attackers now have online stores in which they can purchase services to attack organizations
- While cybersecurity talent is becoming less of an issue among the vendors, at the client level, cybersecurity talent can be difficult to assess and retain
- A new wave of security tools and platforms leveraging AI needs to be understood if the organization wants to reduce the severity of incidents.

Organizations can benefit from outsourcing cyber resiliency services through:

- Using risk analyses performed by vendors to understand the ROI of deploying cybersecurity solutions and procedures for a cost benefit analysis
- 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 and regulations that exist
- Increased understanding of how backups fit into cyber resiliency strategies, and have those backups effectively managed
- An informed workforce that feels more comfortable with cybersecurity, reduces the number of cyber incidents, and can spot a cyber incident in progress to reduce MTTD
- Increased understanding of how to secure legacy applications and bake security by design into digital transformation projects with DevSecOps
- Use of high levels of cybersecurity as a differentiator with clients
- The ability to leverage highly scalable, highly skilled teams when talent is too costly to hire, and to leverage the highly skilled teams for the likes of legal consultancy.

About The Author

Mike is a Senior Analyst and Operations Officer at NelsonHall. His main research focus is on digital transformation technologies, including RPA, blockchain, IoT, artificial intelligence, cognitive, and machine learning.

Highly regarded for his analytical talents, Mike also leads data modeling and analytics initiatives in support of NelsonHall's ITS and BPS market forecasts and market surveys. He was responsible for transforming NelsonHall's extensive global market forecast engine, including the introduction of NelsonHall's unique interactive Self-Forecasting Tool

Mike can be contacted at:

- Email: mike.smart@nelson-hall.com
- Twitter: @MikeS_NH

About NelsonHall

NelsonHall is the leading global analyst firm dedicated to helping organizations understand the 'art of the possible' in digital operations transformation. With analysts in the U.S., U.K., and Continental Europe, NelsonHall provides buy-side organizations with detailed, critical information on markets and vendors (including NEAT assessments) that helps them make fast and highly informed sourcing decisions. And for vendors, NelsonHall provides deep knowledge of market dynamics and user requirements to help them hone their go-to-market strategies. NelsonHall's research is based on rigorous, primary research, and is widely respected for the quality, depth and insight of its analysis.

We would be pleased to discuss how we can bring benefit to your organization. You can contact us via the following relationship manager: Guy Saunders at guy.saunders@nelson-hall.com

Boston
Riverside Center, 275 Grove Street, Suite 2-400, Newton Massachusetts 02466
Phone: +1 857 207 3887

London
Unit 6, Millars Brook,
Molly Millars Lane,
Wokingham, RG41 2AD
Phone: + 44(0) 203 514 7522

Paris
4 place Louis Armand,
Tour de l'Horloge,
75012 Paris
Phone: + 33 1 86266 766