NEAT EVALUATION FOR KYNDRYL:

Cyber Resiliency Services

Market Segments: Overall, Cyber Consulting & Strategy Construction, Incident Response & Backup Services, Managed Cyber Security Services

Introduction

This is a custom report for Kyndryl presenting the findings of the 2022 NelsonHall NEAT vendor evaluation for *Cyber Resiliency Services* in the *Overall, Cyber Consulting & Strategy Construction, Incident Response & Backup Services,* and *Managed Cyber Security Services* market segments. It contains the NEAT graphs of vendor performance, a summary vendor analysis of Kyndryl for cyber resiliency services, and the latest market analysis summary.

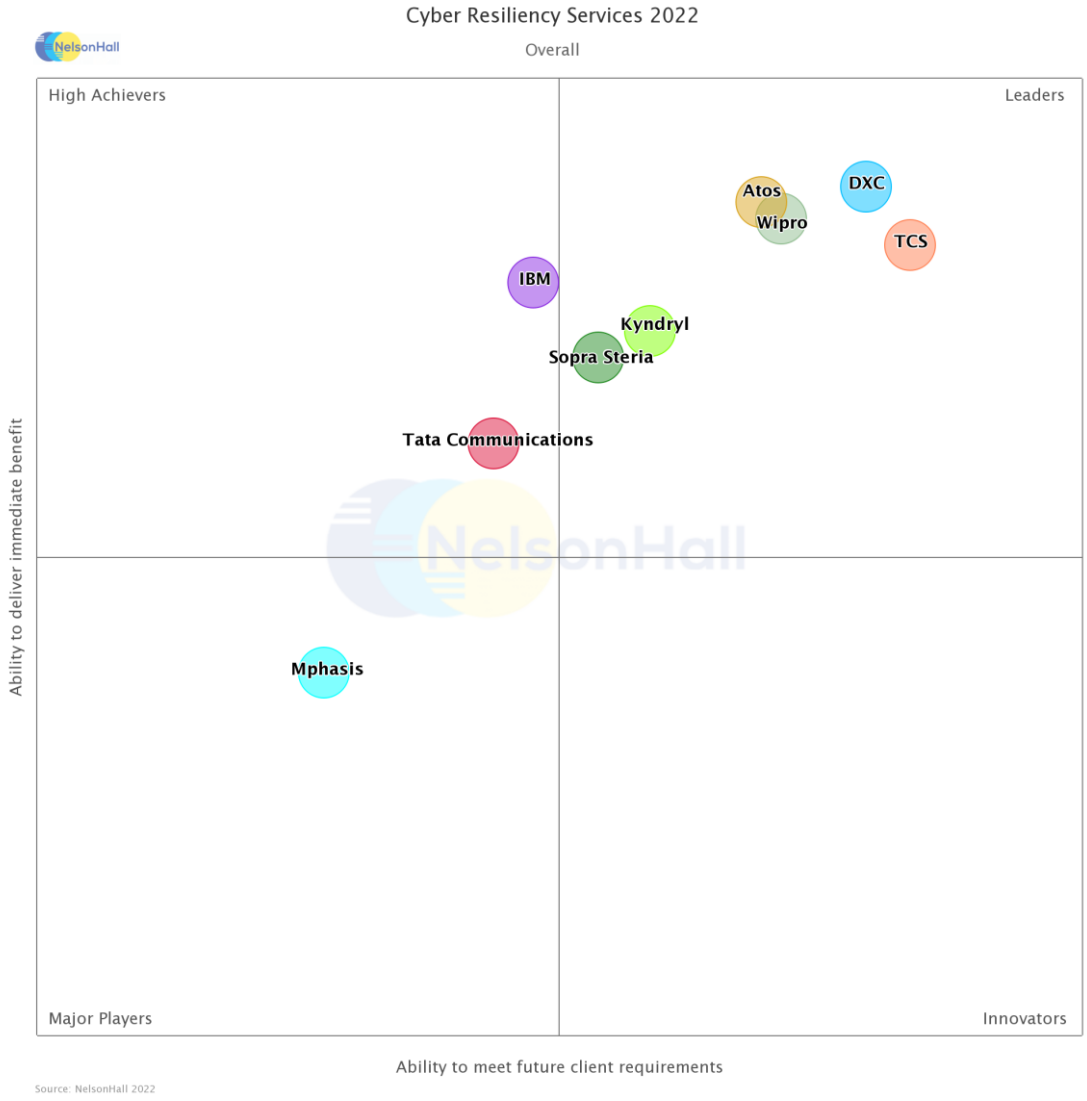
This NelsonHall Vendor Evaluation & Assessment Tool (NEAT) analyzes the performance of vendors offering cyber resiliency services. The NEAT tool allows strategic sourcing managers to assess the capability of vendors across a range of criteria and business situations and identify the best performing vendors overall, and with specific capability in cyber consulting & strategy construction, incident response & backup services, and managed cyber security services.

Evaluating vendors on both their 'ability to deliver immediate benefit' and their 'ability to meet future client requirements', vendors are identified in one of four categories: Leaders, High Achievers, Innovators, and Major Players.

Vendors evaluated for this NEAT are: Atos, DXC Technology, IBM, Kyndryl, Mphasis, Sopra Steria, Tata Communications, TCS, and Wipro.

Further explanation of the NEAT methodology is included at the end of the report.

NEAT Evaluation: Cyber Resiliency Services (Overall)

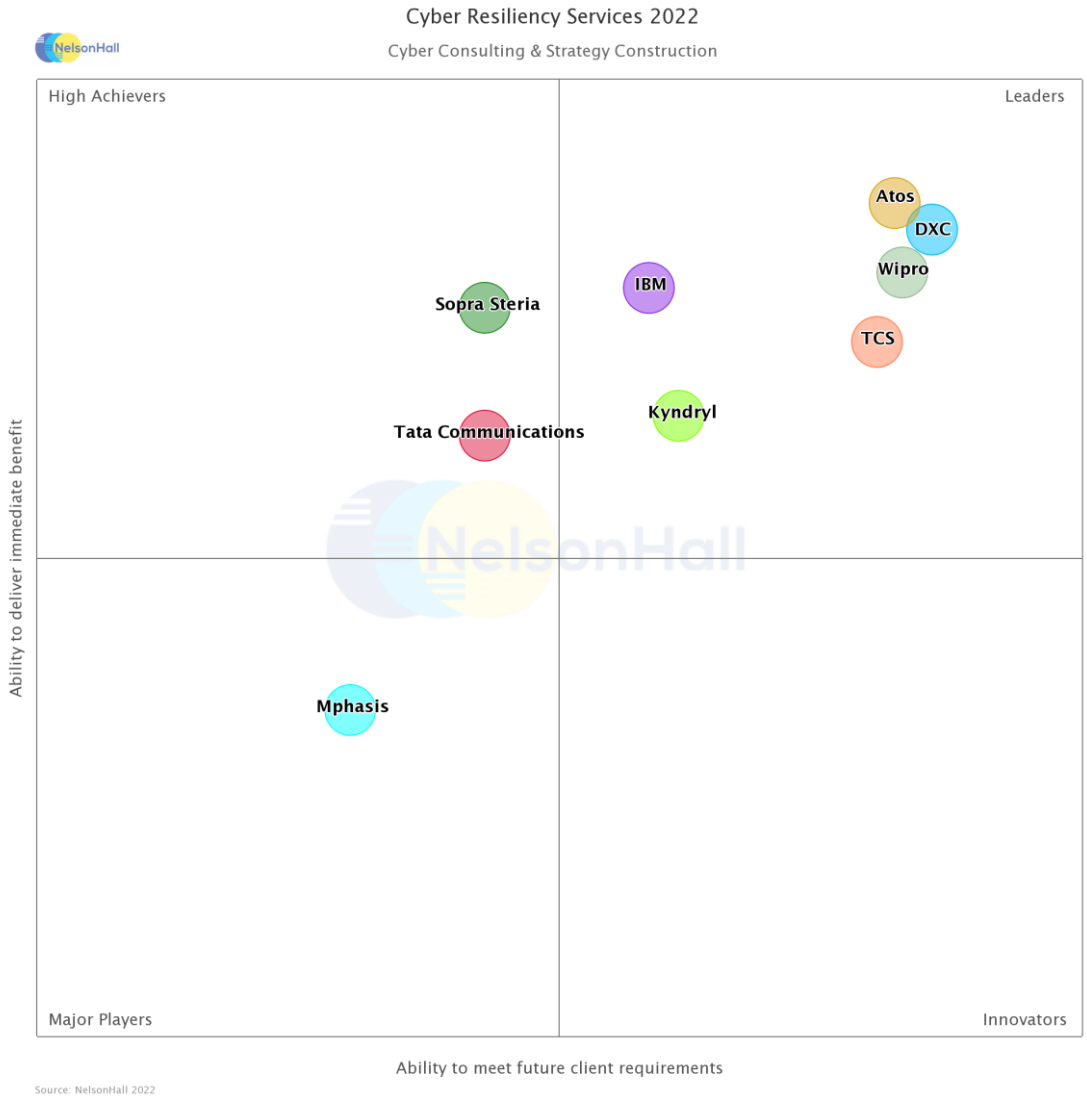


NelsonHall has identified Kyndryl as a Leader in the *Overall* market segment, as shown in the NEAT graph. This market segment reflects Kyndryl's overall ability to meet future client requirements as well as delivering immediate benefits to its cyber resiliency clients.

Leaders are vendors that exhibit both a high capability relative to their peers to deliver immediate benefit and a high capability relative to their peers to meet future client requirements.

Buy-side organizations can access the *Cyber Resiliency Services* NEAT tool (*Overall*) here.

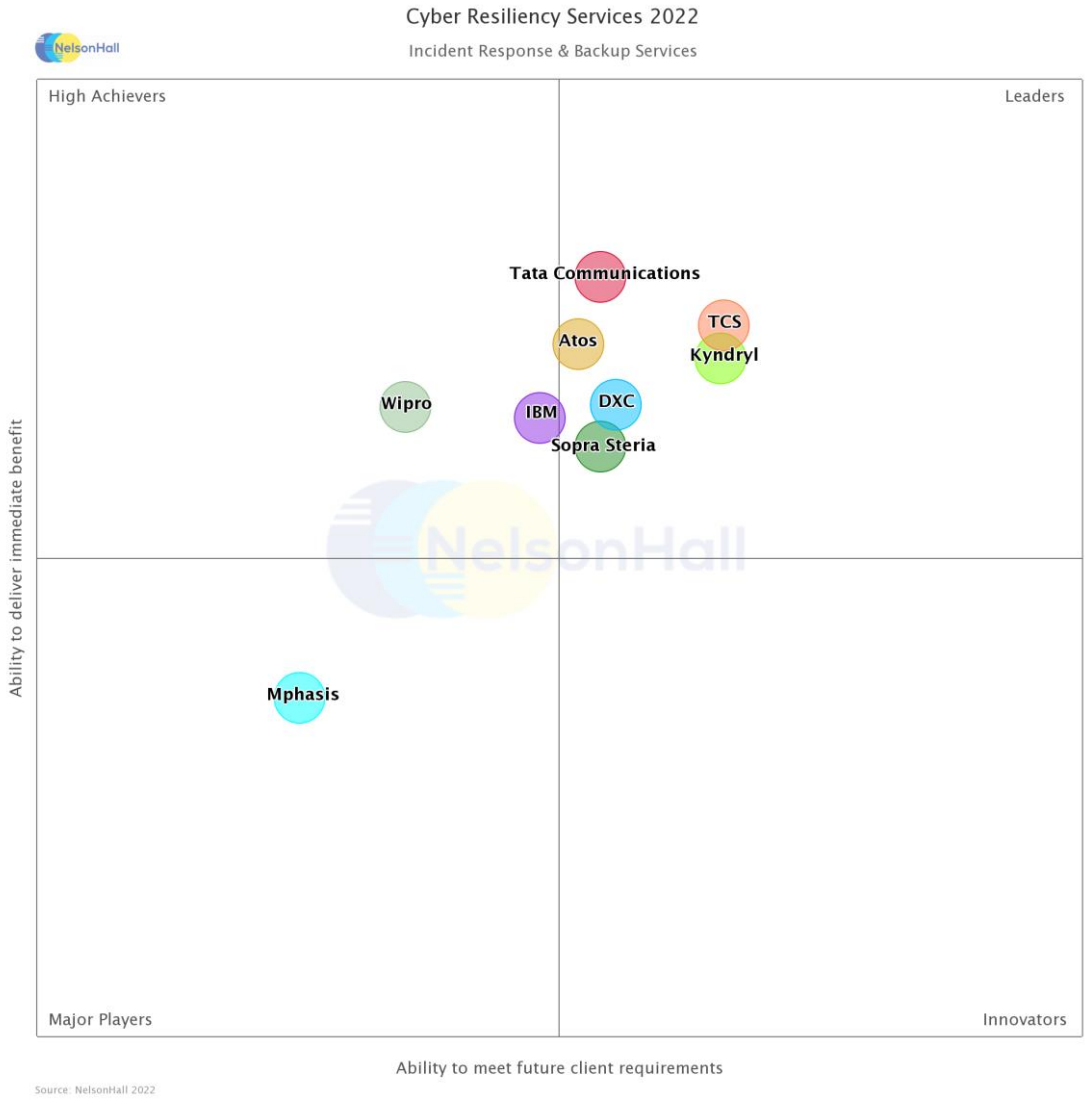
NEAT Evaluation: Cyber Resiliency Services (Cyber Consulting & Strategy Construction)



NelsonHall has identified Kyndryl as a Leader in the *Cyber Consulting & Strategy Construction* market segment, as shown in the NEAT graph. This market segment reflects Kyndryl's ability to meet future client requirements as well as delivering immediate benefits to its cyber resiliency clients with specific capability in cyber consulting and strategy construction.

Buy-side organizations can access the *Cyber Resiliency Services* NEAT tool (*Cyber Consulting & Strategy Construction*) here.

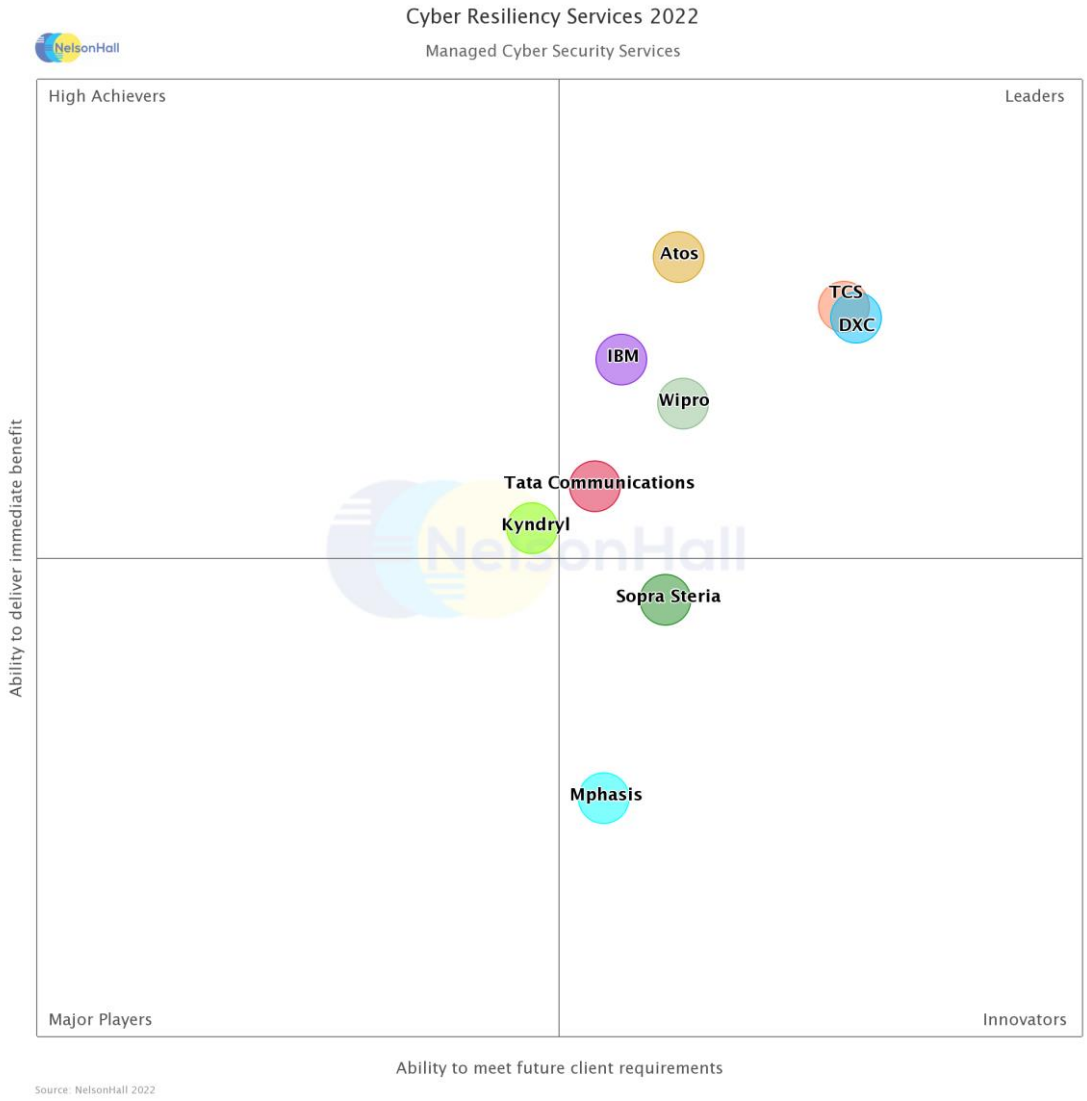
NEAT Evaluation: Cyber Resiliency Services (Incident Response & Backup Services)



NelsonHall has identified Kyndryl as a Leader in the *Incident Response & Backup Services* market segment, as shown in the NEAT graph. This market segment reflects Kyndryl's ability to meet future client requirements as well as delivering immediate benefits to its cyber resiliency clients with specific capability in incident response and backup services.

Buy-side organizations can access the *Cyber Resiliency Services* NEAT tool (*Incident Response & Backup Services*) here.

NEAT Evaluation: Cyber Resiliency Services (Managed Cyber Security Services)



NelsonHall has identified Kyndryl as a High Achiever in the *Managed Cyber Security Services* market segment, as shown in the NEAT graph. This market segment reflects Kyndryl's ability to meet future client requirements as well as delivering immediate benefits to its cyber resiliency clients with specific capability in managed cyber security services.

High Achievers are vendors that exhibit a high capability relative to their peers to deliver immediate benefit but have scope to enhance their ability to meet future client requirements.

Buy-side organizations can access the *Cyber Resiliency Services* NEAT tool (*Managed Cyber Security Services*) here.

Vendor Analysis Summary for Kyndryl

Overview

Kyndryl organizes cyber resiliency into four main service domains: security assurance services, zero trust services, security operations & response services, and incident recovery services. The majority of Kyndryl's cyber resiliency services reside in its incident recovery services.

Kyndryl's cyber incident recovery services include:

- Cyber incident recovery for the mitigation of disasters and cyber incidents: services to help identify risks to the client's infrastructure and data and support them in building a more resilient infrastructure. The cyber incident recovery consulting service evaluates the client across 100 controls to understand the current state of resiliency and the client's target state. During or after a cyber attack, Kyndryl offers data and platform recovery for IBM platforms, Azure, Dell EMC, GCP, VMware, and Cisco. Kyndryl states that integrating its orchestration software into the cyber incident recovery service can reduce the downtime resulting from an incident by 80%
- Managed backup services: Kyndryl primarily partners with backup solution providers and has standard offerings using IBM Spectrum Protect, Veeam, Veritas, and Commvault
- In Kyndryl's backup services, all client data is air-gapped to prevent cyber-attackers from moving across the network and infecting backups. All backups are subject to AI-based anomaly detection. This is based on IBM research and, rather than using signature-based anomaly detection, uses heuristics-based detection
- Hybrid platform recovery: Kyndryl’s resiliency block replicator allows hybrid platform recovery and cyber incident recovery. The recovery platform has 900 libraries supporting on-premise and cloud
- Datacenter facilities to design and build optimized datacenters with a focus on building resiliency while lowering the total cost of ownership.

Financials

NelsonHall estimates that cyber resilience-related services account for ~13% of Kyndryl's overall business, or $2.4bn.

Strengths

- Kyndryl states that through its cyber incident recovery services, it can minimize the downtime of an organization by up to 80%
- Infrastructure management expertise, in particular orchestration capabilities using acquired Sanovi technologies. As part of a cyber resiliency service, the orchestration capabilities are fundamental to Kyndryl’s backup and recovery and SOAR capabilities
- Strong partnerships supporting managed cybersecurity services.

Challenges

- In cyber resiliency, Kyndryl's primary focus is on the recovery after a cyber incident rather than reducing cyber incidents in the first place. While a focus on reducing the number of cyber incidents does not allow an organization to hold back on preparing to recover from an incident, it can reduce the total impact of cyber threats
- While Kyndryl states that its differentiator in the digital identity space is its ability to stitch together the security point solutions during a systems integration project, many cyber resiliency vendors have this focus, and modern cyber resiliency platforms are increasingly designed to be easy to integrate
- Kyndryl is building several cybersecurity services currently supported through partnerships, where Kyndryl has no control over the delivery or development of the service.

Strategic Direction

Following its spin-off from IBM, Kyndryl is building supplementary cyber resiliency services to augment its strength in the backup and recovery space which currently account for the majority of the company's cyber-related services. A substantial portion of Kyndryl's zero trust and security operations center services is currently supported through white-labeled services from IBM. However, the company aims to develop independent services in the next two years. When developing these zero trust and security operations center services, the company focuses on delivering an automation-focused and plug-and-play service under the Kyndryl platform strategy.

As these services develop, Kyndryl states that the advantage of Kyndryl over IBM Security Services is that the company is not locked into IBM security technologies and can support security operations center services using tools from several partners including but not limited to Splunk, Sentinel, etc.

When competing against the cloud providers offering backup and recovery services, Kyndryl's positioning (unlike the cloud providers) is its focus beyond cloud platform configuration backup. This includes data, application, and business process recovery, and through integration services or white-labeled managed services also provides broader cybersecurity services.

In presenting its services to clients, Kyndryl is working on building out its commercial capabilities to provide more of its services through direct sales rather than partner sales, following the split from IBM.

Kyndryl is also investigating developing a retainer-based recovery service, as it has witnessed that cyber response services often stop before providing services to support a client in recovering its data.

Outlook

As the spin-off from IBM's infrastructure services business, Kyndryl has a wealth of experience in supporting large enterprises in designing and managing legacy and cloud-based infrastructure estates. The technology acquired with Sanovi can support cyber resiliency operations through orchestrating the response to disasters or cyber-related incidents.

More traditional cybersecurity services such as MDR, IAM, and application security remained with IBM Security. Kyndryl is in the process of building capabilities to support some of these services and is reliant on partners to provide such services during this development.

Despite Kyndryl offering some zero trust and security assurance services, the majority of Kyndryl's cyber resiliency services lie within its data backup and governance services.

Cyber Resiliency Services Market Summary

Overview

Cyber resiliency is becoming an increasingly critical issue for organizations as the value and amount of data collected and held increases. Whereas in the past, organizations may simply have focused on meeting compliance and securing data through cybersecurity, these same organizations must now adopt the view that, at some point, they will be breached. Therefore, organizations should look at measures to make data access more difficult and reduce the availability of data (even within the context of a cyber breach) and ensure they can continue operations within the shortest timespan possible.

All organizations need to improve their level of cyber resiliency. Illustrating this point, two cyber resiliency services vendors suffered cyber attacks in the last 12 months: Sopra Steria and Cognizant. Both companies had large-scale cyber resiliency plans in place and the adherence to these plans undoubtably reduced the impact of the breaches. This is not to say that these companies had inadequate cyber resiliency strategies; instead, that cyber resiliency has an element of cost-risk analysis and cyber strategies always have room for improvement.

Buy-Side Dynamics

Key challenges for organizations looking to outsource cyber resiliency services are:

- A lack of understanding of the requirements for cyber resilience, with organizations focused on the technical aspects of preventing, detecting, and responding to a cyber incident
- Difficulty in measuring the effectiveness of a cyber resiliency strategy before a cyber attack takes place
- Focus on the speed of transformation and the introduction of next-generation technologies such as IoT, RPA, and blockchain thereby increasing the attack surface area
- Even during transformations, organizations hold a large number of legacy applications which require heavy investment to patch in order to meet standards, and can pose more of a challenge to track cyber security information
- Difficulty in deciding what data needs to be backed up and the level of MVB to fall back to in the event of cyber attack, and the difficulty in matching backup requirements to regulatory requirements such as GDPR
- A low level of cyber skills within organizations and difficulty in training these skills decreases the chance that employees will detect indicators of compromise, increasing the dwell time and the overall mean-time-to-respond
- An increasing number of regulations that carry the risk of higher fines
- Increasing ease and sophistication of attacks. Attackers only have to succeed in an attack once, whereas the client must aim to successfully detect and resolve all cyber incidents; attackers have online stores in which they can easily purchase services to attack organizations. At the same time, more sophisticated attackers are leveraging AI/ML to perform attacks which are harder to defend against
- Data subjects becoming more aware of cyber resiliency and wanting their data to be properly secured, while organizations are looking to collect and store more client data.

Success Factors

Critical success factors for vendors within the cyber resiliency services market are:

- Ability to work with partners (or for end-to-end providers to utilize other business units) to introduce cyber resiliency upfront as a differentiator for clients
- Ability to work across the client's business operations, IT, and third parties
- Ability to build a cyber resiliency consulting capability, either with strong in-house training to leverage existing industry specific knowledge or through acquisitions
- Strong research capability to track cyber resiliency regulations and the impact of cyber digital technologies such as IoT, AI/ML, blockchain, and quantum. Whereas all vendors have this research to some degree, the more advanced technologies such as quantum and the development of quantum encryption are only covered by a small percentage of the vendors analysed and will be critical to all organizations going forward
- Ability to build or assess the security IP and platforms for new resiliency services, for example SOAR platforms, platforms to assess the data security requirements of the client, native cloud security platforms, and platforms to assess third-party risk
- Maintaining commoditized traditional security services while building advanced security services and maintaining margins through the use of automation
- Ability to improve the level of cyber awareness within the organization
- Developing in-country capabilities to support security services such as advanced cyber forensic analysis
- Demonstrating ROI and increasing overall return on investment for the client by leveraging existing investments containing native security controls.

Outlook

Over the next five years:

- Growth in cyber resiliency services will be led by consulting services and IR & backup services accounting for more than 55% of the market
- Despite withdrawing the Indian Personal Data Protection Bill 2019, which was set to significantly boost market sizes in the region, APAC is the fastest growing region, with a 30% CAGR. Additionally, it is predicted that a new personal data privacy act will be developed during the period
- Strategies will focus on reducing the impact of cyber incidents, and will include reducing reputational damage, cybersecurity insurance services, fallback IT systems and AI to detect user actions that detect inflated privileges, and users and automations acting outside normal parameters
- NelsonHall expects (in the next three years) to see the key areas of investment to be BCM plans, SOAR and security for automation, verticalized security offerings, and quantum security. Growth in these segments will be supported by increasing adoption of digital technologies such as cloud, IoT/OT, blockchain, AI/ML, the metaverse, and quantum computing, alongside new cyber security regulations. Cyber as an integral part of BCM plans in particular will lead to the development of MVB strategies for cyber with fallback positions, reducing the time for organizations to recover from incidents

- As organizations will be more cloud-based and hold less legacy architecture, and as cloud-native security tools are naturally more agile, the time and cost to implement security tools will reduce, further shifting focus to upfront and ongoing consulting services
- Manufacturing and retail industries will shift to capture more customer data, incorporate more IoT/IoE, and shift to an aaS model for products, supporting growth over the period as these organizations become more of a target for cyber attackers
- When available, data backup teams will work directly with cyber resiliency teams as backup services become standardized, particularly in regulated industries.

NEAT Methodology for Cyber Resiliency Services

NelsonHall's (vendor) Evaluation & Assessment Tool (NEAT) is a method by which strategic sourcing managers can evaluate outsourcing vendors and is part of NelsonHall's *Speed-to-Source* initiative. The NEAT tool sits at the front-end of the vendor screening process and consists of a two-axis model: assessing vendors against their 'ability to deliver immediate benefit' to buy-side organizations and their 'ability to meet client future requirements'. The latter axis is a pragmatic assessment of the vendor's ability to take clients on an innovation journey over the lifetime of their next contract.

The 'ability to deliver immediate benefit' assessment is based on the criteria shown in Exhibit 1, typically reflecting the current maturity of the vendor's offerings, delivery capability, benefits achievement on behalf of clients, and customer presence.

The 'ability to meet client future requirements' assessment is based on the criteria shown in Exhibit 2, and provides a measure of the extent to which the supplier is well-positioned to support the customer journey over the life of a contract. This includes criteria such as the level of partnership established with clients, the mechanisms in place to drive innovation, the level of investment in the service, and the financial stability of the vendor.

The vendors covered in NelsonHall NEAT projects are typically the leaders in their fields. However, within this context, the categorization of vendors within NelsonHall NEAT projects is as follows:

- Leaders: vendors that exhibit both a high capability relative to their peers to deliver immediate benefit and a high capability relative to their peers to meet future client requirements
- High Achievers: vendors that exhibit a high capability relative to their peers to deliver immediate benefit but have scope to enhance their ability to meet future client requirements
- Innovators: vendors that exhibit a high capability relative to their peers to meet future client requirements but have scope to enhance their ability to deliver immediate benefit
- Major Players: other significant vendors for this service type.

The scoring of the vendors is based on a combination of analyst assessment, principally around measurements of the ability to deliver immediate benefit; and feedback from interviewing of vendor clients, principally in support of measurements of levels of partnership and ability to meet future client requirements.

Note that, to ensure maximum value to buy-side users (typically strategic sourcing managers), vendor participation in NelsonHall NEAT evaluations is free of charge and all key vendors are invited to participate at the outset of the project.

Exhibit 1

'Ability to deliver immediate benefit': Assessment criteria

Assessment Category	Assessment Criteria
Offerings	Consultancy services Consultancy services for business continuity planning Cyber related legal consulting Compliance consultancy and management services Managed security services for networks and/or infrastructure Managed security services for applications and end users computing Digital Identity services Incident response services Backup and recovery services
Delivery Capability	Use of security accelerators Ability to reevaluate resiliency posture at regular intervals Feedback provided by the vendor Dashboard capabilities Identification of key assets/personnel vendor bringing best practice and innovation ideas Cyber resiliency delivery capability – North America Cyber resiliency delivery capability - U.K. Cyber resiliency delivery capability - Continental Europe Cyber resiliency delivery capability – Rest of EMEA Cyber resiliency delivery capability - APAC Cyber resiliency delivery capability - LATAM
Benefits Achieved	Overall performance Ability to respond to threats Ability to spread cybersecurity awareness throughout the organization Reduction in number of incidents Ability to reimagine service/process Strength of partnership Flexibility Value for money

Exhibit 2

'Ability to meet client future requirements': Assessment criteria

Assessment Category	Assessment Criteria
Level of Investments	Level of investment in Consultancy services
	Level of investment in Consultancy services for business continuity planning
	Level of investment in Managed security services for networks and/or infrastructure
	Level of investment in Managed security services for applications and end users computing
	Level of investment in Digital Identity services
	Level of investment in Incident response services
	Level of investment in Backup and recovery services
	Overall

For more information on other NelsonHall NEAT evaluations, please contact the NelsonHall relationship manager listed below.

research.nelson-hall.com

Sales Inquiries

NelsonHall will be pleased to discuss how we can bring benefit to your organization. You can contact us via the following relationship manager:

Darrin Grove at darrin.grove@nelson-hall.com