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 2024 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.

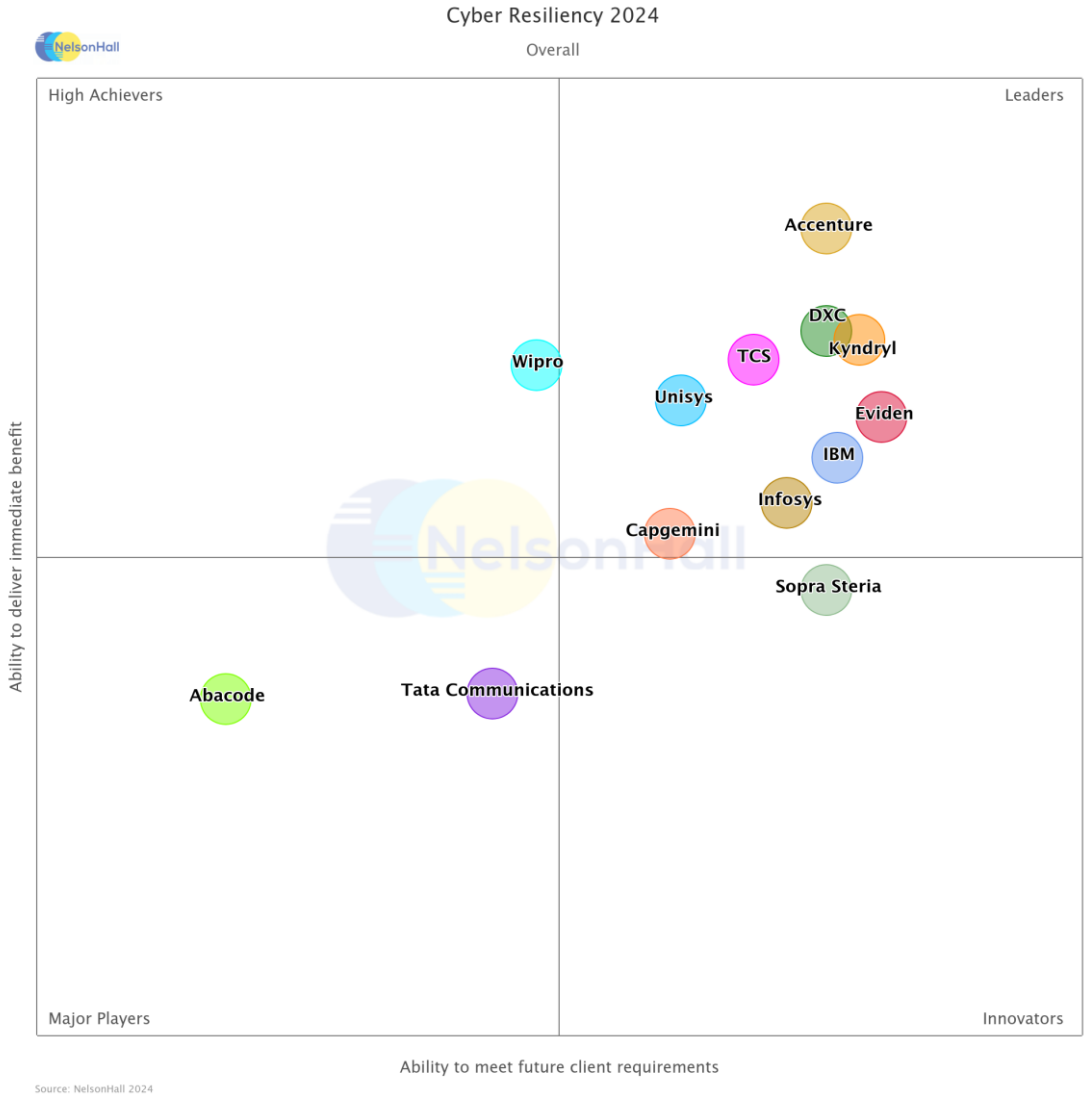
This NelsonHall Vendor Evaluation & Assessment Tool (NEAT) analyzes the performance of vendors offering cyber resiliency services. The NEAT tool allows strategic sourcing managers to assess the capability of vendors across a range of criteria and business situations and identify the best performing vendors 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: Abacode, Accenture, Capgemini, DXC Technology, Eviden, IBM, Infosys, Kyndryl, Sopra Steria, Tata Communications, TCS, Unisys, and Wipro.

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

# NEAT Evaluation: Cyber Resiliency Services (Overall)

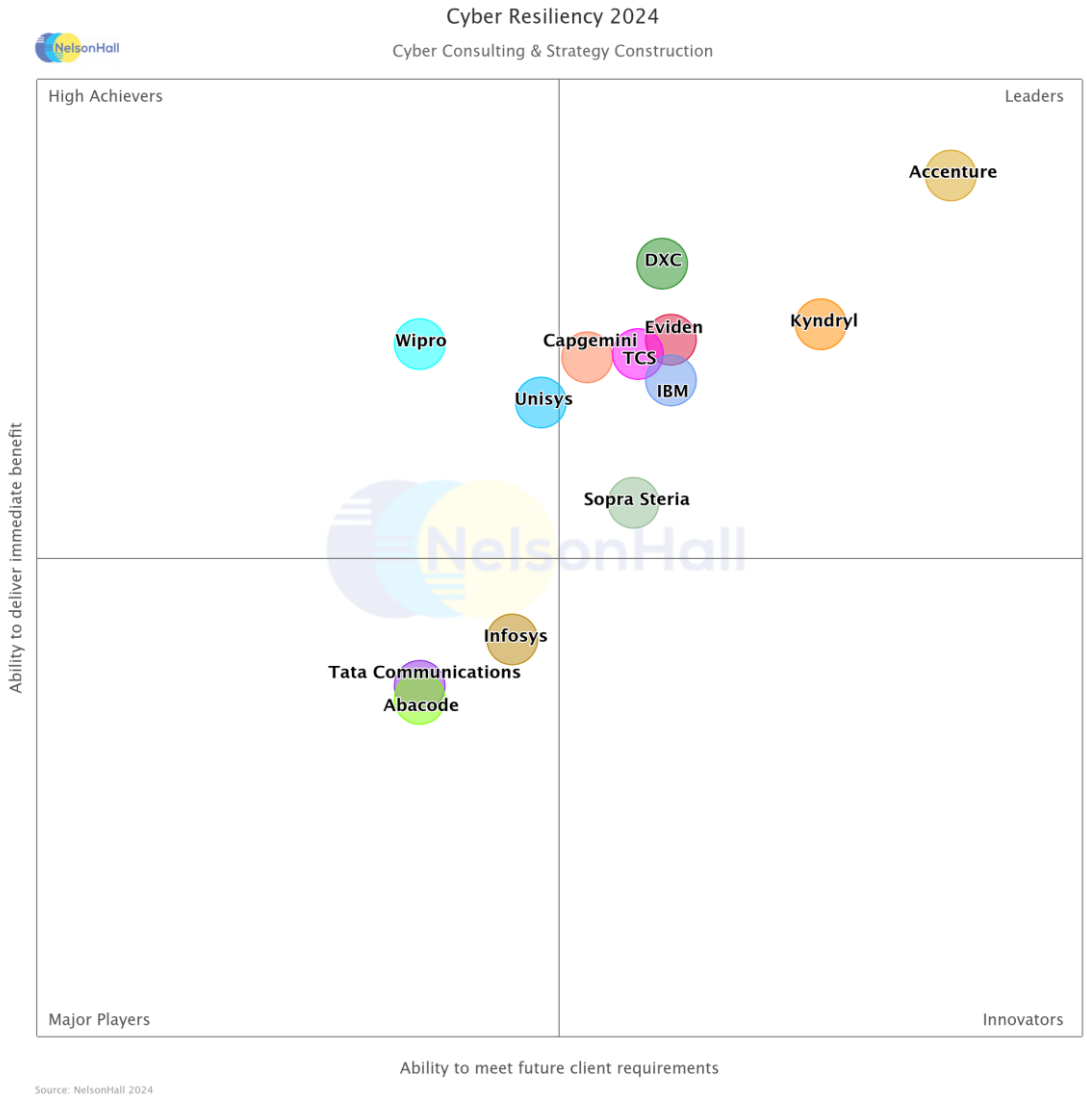



NelsonHall has identified Kyndryl as a Leader in the *Overall* market segment, as shown in the NEAT graph. This market segment reflects Kyndryl's overall ability to meet future client requirements as well as delivering immediate benefits to its cyber resiliency clients.

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.

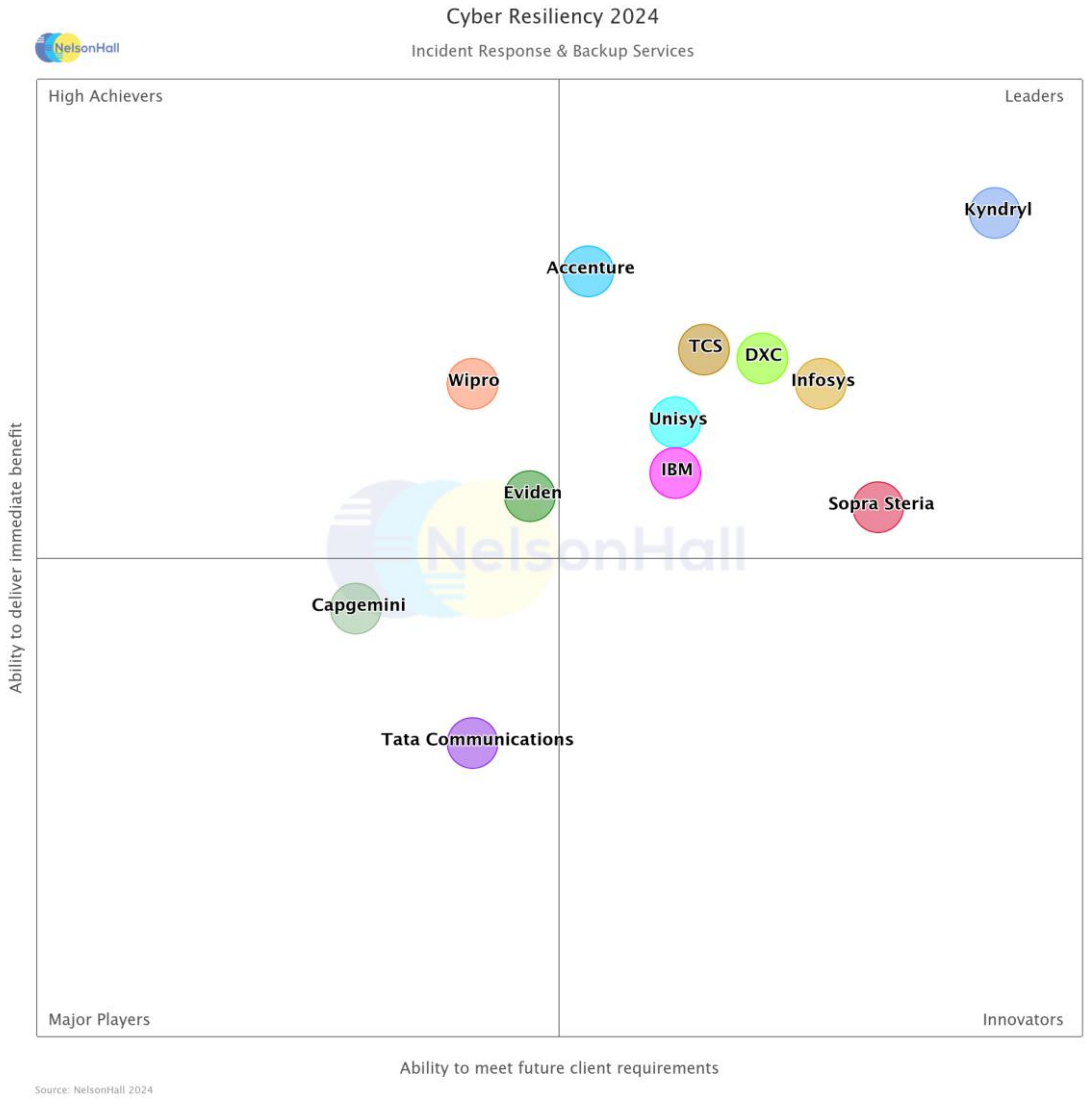
# NEAT Evaluation: Cyber Resiliency Services (Cyber Consulting & Strategy Construction)




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.

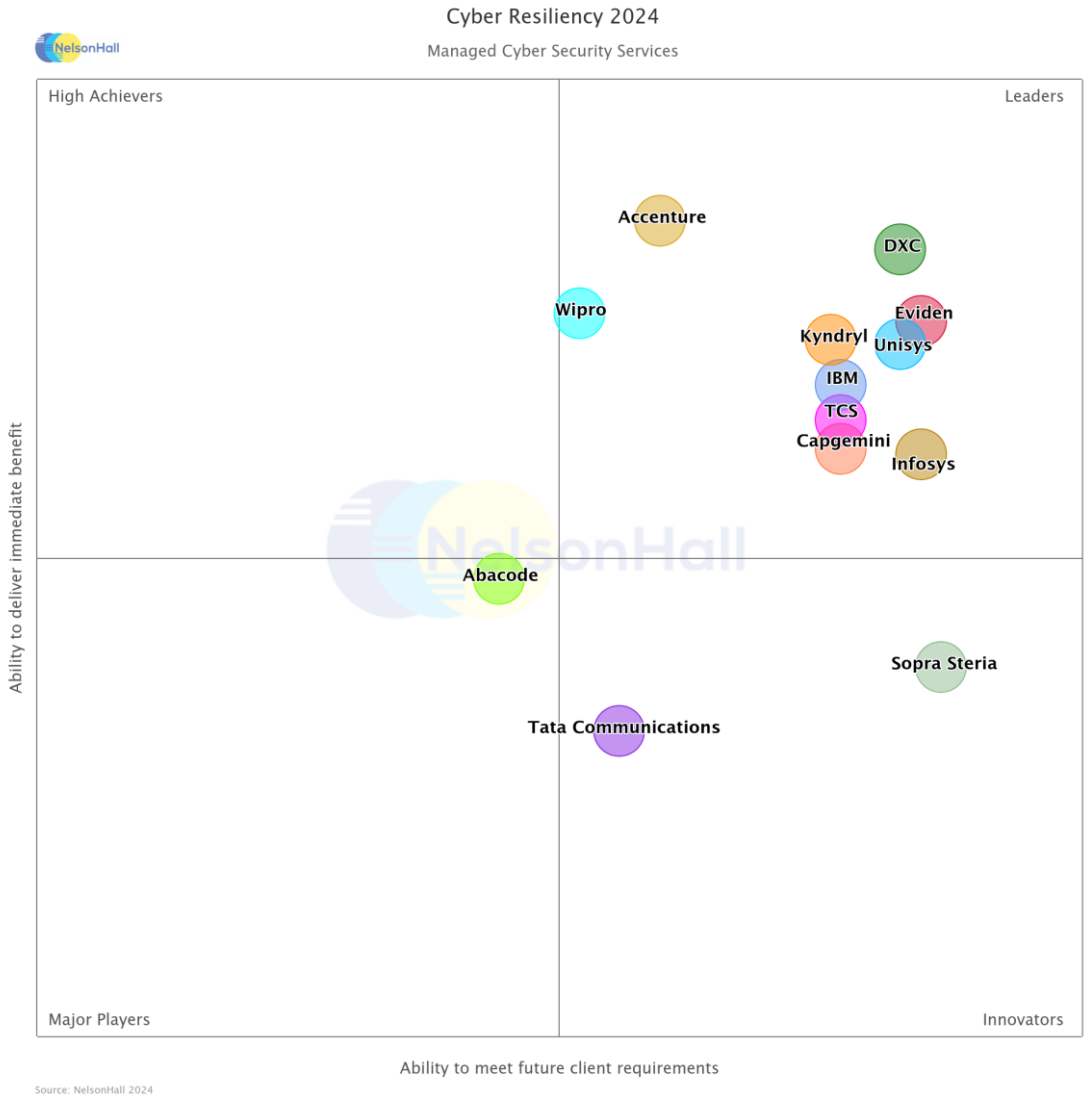
# NEAT Evaluation: Cyber Resiliency Services (Incident Response & Backup Services)




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 Leader 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.

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

# Vendor Analysis Summary for Kyndryl

## Overview

Kyndryl organizes a portfolio of cyber resiliency services which have the ability to anticipate, protect, withstand, respond, and recover from any adverse condition, including a cyber outage. The portfolio is divided into four main service domains: security assurance services, zero trust services, security operations and response services, and incident recovery services:

- *Security assurance services* – these services help organizations maintain compliance in their application and infrastructure security policies and controls. These services aim to test and certify the client's resiliency strategy concerning data and application backup and recovery, and provide ongoing management of this compliance. Security assurance services include security, strategy, and risk management, offensive security testing, and compliance management
- *Zero trust services* – these services include identity and access management (IAM), endpoint security, network security, application and workload security, and data protection and privacy. Kyndryl's IAM implements its zero-trust Identity and Access Governance (IAG) framework. Within this space, Kyndryl detects inflated privileges and performs next generation User and Entity Behavior Analytics (UEBA). Zero trust services include IAM services, endpoint security, network security, and data protection and privacy
- *Security operations and response services* – Kyndryl provides security operations using its Security Operations as a Platform (SOaaP) built on top of Kyndryl Bridge to provide MDR services. Kyndryl's security operations and response services include advanced threat detection, incident response and forensics, security operations center services, and vulnerability management
- *Incident recovery services* – Kyndryl offers a range of services to support resiliency goals before, during, and after cyber-attacks, including services that enable data and platform vaulting, anomaly detection, run book development, testing, and recovery. Client engagement typically begins with a consultant helping customers build their strategy, map the minimum viable business, and select appropriate technologies (e.g., Veeam, Dell, Veritas, Cohesity, Rubrik, Broadcom). Services include cyber incident recovery, managed backup services, hybrid platform recovery, data center design, and business and IT resiliency consulting.

Across the four service domains, Kyndryl offers advice, implementation, and run services, with run services being by far the largest of these categories.

Kyndryl has ~7.5k employees delivering cyber resiliency services across 63 countries, including 2.5k consultants providing security advisory services.

The company has ~3k patents in the IT Risk Management space, 500 of which are associated with the Cyber Incident Recovery domain.

Kyndryl's security offerings are supported through a network of four global and four regional Security Operation Centers (SOC), and two remote support centers.

## Financials

NelsonHall estimates that Kyndryl's security and resiliency revenues for CY 2023 were ~$2.1bn, equivant to ~13% of the company's overall revenue.

The overall security and resiliency business has boasted consistent double-digit growth y/y, with security operations and response being the fastest growing segment.

## Strengths

- Strong incident recovery services specialty. Kyndryl has stated that through its cyber incident recovery services, it can minimize the downtime of an organization by up to 80%
- As part of a cyber resiliency service, its orchestration and infrastructure management expertise is fundamental in Kyndryl's backup and recovery and SOAR capabilities. The company's incident recovery services leverage these orchestration capabilities
- In transitioning away from IBM, Kyndryl has launched a new suite of services including its Security Operations as a Platform (SOaaP) that enables increased flexibility through a modular approach to third-party security solutions, and lower MTTR threats through automation.

## Challenges

While Kyndryl states that its differentiator is the ability to stitch together the security point solutions leveraging its Kyndryl Bridge platform, many security vendors have this focus and are increasingly leveraging third-party solutions or building security data lake solutions with supporting integration management.

## Strategic Direction

Aligned to the company strategy, Kyndryl's cyber resilience team has launched new services and secured partnerships to support its portfolio, in addition to continuing to develop its talent and delivery network. Services supporting clients meeting DORA regulations have garnered client interest, with more than 20 banking clients being supported through advisory services.

The company has found that an increasingly important value proposition is demonstrating the ROI of its security solutions, not only against the probability of a cyber incident, but against its industry peers.

The company's investments in AI to defend clients include its partnership with Microsoft, which is being applied to support security analysts in threat hunting, threat dossier creation, digital forensics, and creating legal note summaries to security incidents.

We expect the company to continue to build out new services including:

- Services to bring together more technologies together with Kyndryl Bridge with an overarching governance framework and further deployments of instrumentation within the cyber operations platform
- Increased support for operational technology (OT) security services

- The integration of GenAI into the solutions. Kyndryl has partnered with Microsoft for access to Microsoft 365 Copilot, Azure OpenAI, and Microsoft Fabric within its service portfolio.

## Outlook

Following the split with IBM, Kyndryl has been heavily investing in developing new services, IP, partners and resources. While continuing to develop the Kyndryl brand, it is also replacing subcontracted managed security services.

The major strengths within the business are its large consulting presence of ~2.5k consultants holding ~7.7k certifications and accreditations, and numerous frameworks to support clients in maximizing their cyber resiliency maturity; its Kyndryl Bridge IP to enable the integration of third-party cyber data and sources; and the company's experience in responding to and recovering from cyber events.

# Cyber Resiliency Services Market Summary

## Overview

Cyber resiliency services are crucial to supporting an organization's operations through a proactive approach to anticipating, protecting, withstanding, and recovering from cyber events and meeting various cyber-related regulations. This, along with models such as zero-trust, helps ensure that when organizations are inevitably targeted by threat actors, the impact of attacks is minimized.

Still, organizations are unable to keep up with best practices and regulations, and with technologies such as GenAI (both for its use in and outside of cybersecurity), while remaining cost-competitive. Third-party cyber resiliency services are offered by a mix of IT services providers, network communication providers, and consultancies.

## Buy-Side Dynamics

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

- Shifting left when it comes to security resiliency. For example, through the creation of security by design and SBOM which can then be used for ongoing vulnerability management with patch management, or through bringing MVB, zero trust, and other cyber resiliency strategies upfront in digital transformation discussions
- Keeping abreast of changing cybersecurity and data privacy regulations across all geographies and industries
- Keeping abreast of the impact of new technologies such as GenAI, IoT, AI/ML, blockchain, and quantum computing, covering both the use of the technologies for the client and by the attacker. In particular, AI as part of security data lake solutions that help identify indicators of compromise, relate this information to cyber analysts, and suggest next best actions
- Continuously detecting and managing vulnerabilities in client third-party relationships such as the client's supply chain, and aiding clients in remaining compliant by notifying third parties during cyber events
- Targeting advanced security services and transitioning away from commoditized traditional cybersecurity services before these services become business-as-usual offerings. As an example, DDoS is now a standard offering within cloud infrastructure platforms
- Assisting organizations in leveraging security features in previously invested platforms. In particular, assessing existing cyber resiliency solutions that are deployed for overlapping features and unused licenses; this may take the form of increased use of native cloud security tools, IAM through O365 licenses, or removing legacy security tools. This work helps improve the ROI within cyber resiliency engagements, assessed through the NIST-certified FAIR model
- Educating client employees to be aware of cyber resiliency and flag indicators of compromise as solutions (such as GenAI) when used by threat actors, make these attacks harder to detect.

## Market Size & Growth

The current cyber resiliency services market is worth $28.6bn and is set to grow at more than 11% CAGR to reach $44.3bn by 2027.

In the U.S., state-by-state regulatory requirements will not necessarily be the growth engines, as U.S. organizations generally are set up to meet these requirements, supporting customers across state lines. Instead, federal legislation covering OT/IoT, GenAI, and SEC-based regulations, etc. can be expected to support this growth.

In other geographies, EU's DORA and NIS2 Directives, and India's Digital Personal Data Protection Act 2023 will support immediate growth, with later year growth supported by new digital technology advancements.

The manufacturing and retail industries shifting to capture more customer data, incorporate more IoT/IoE, and shifting to an as-a-Service model for products, increases the likelihood that they become targets for bad actors and increase the requirement to improve resiliency.

Demand for cyber resiliency services from the financial services industries will be driven by their heavy investment in implementing defenses against the threat of quantum computing breaking existing encryption methods.

## Success Factors

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

- The ability to work across the client's business operations, IT, and third parties
- The ability to increase the frequency of security assessments to move towards continuous assessments and compliance to reduce the attack surface and third-party risk
- Keeping track of cyber regulations and building playbooks and frameworks to support clients in meeting these requirements and implementing these controls in a quick and cost-effective manner
- Internal and external research coverage to track developments within the GenAI, IoT/OT, AI/ML, blockchain, and quantum technologies, how they are being deployed by clients, and security requirements for these digital transformation projects
- Deploying security mesh technologies, which reduces the effort required to connect security technologies and collect security data from these technologies into a central data lake for analysis that can better support the identification of advanced persistent threats
- Deploying AI/ML and GenAI technologies within MDR to reduce the toil required to sort through this increase of data from security mesh technologies, identify indicators of compromise, and provide next-best actions
- Being able to prove the ROI of cyber resiliency services, through use of the NIST FAIR model at the start of the contract, then continuously improving this ROI through license cost optimization, replacing legacy solutions, and automation within security tools while retaining managed security services revenues and margins
- New tools and techniques to support client employees in identifying new phishing techniques and to increase the level of general cyber awareness
- Maintaining commoditized traditional security services while building advanced security services and maintaining margins through the use of automation.

## Outlook

Over the next five years, NelsonHall expects to see:

- BCM plans to be built into cybersecurity as a standard, in particular, to prepare clients for SOAR
- An increasing range of consultancy services to include the security of GenAI solutions
- Solutions to better support phishing attempts as GenAI is used to create more convincing phishing work, against which general cyber awareness will not be enough to secure
- As GenAI solutions prove themselves in providing next-best actions, there will be an adoption of these solutions into SOAR, with humans taking final decisions to run GenAI-suggested workflows
- IAM advancements will relate to user experience, support for the metaverse, and government policies for the digitalization of services
- Biometric authentication by default and AI to detect inflated privileges
- A general rising move from role-based access control (RBAC) to attribute-based access control (ABAC) deployments
- There will be a tighter hold of contractual agreements and regulations within the cyber platform, which can be reported against cyber incidents in support of reporting to third-party stakeholders and regulatory authorities
- The normalized use of OCR/NLP/AI to ingest regulatory requirements and responses from third parties will normalize the controls and monitor compliance.

# 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 future client 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 future client 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<br>Business Continuity Planning<br>Cyber related legal consulting<br>Compliance consultancy and management services<br>Managed security for networks/infrastructure<br>Application security services<br>Digital identity services<br>Incident response services<br>Backup and recovery services |
| Delivery Capability | Use of security accelerators<br>Ability to reevaluate resiliency at regular intervals<br>Application of AI/ML to reduce risks, support cybersecurity employees, and respond to threats<br>Cyber resiliency delivery capability – North America<br>Cyber resiliency delivery capability – U.K.<br>Cyber resiliency delivery capability – Continental Europe<br>Cyber resiliency delivery capability – Rest of EMEA<br>Cyber resiliency delivery capability – APAC<br>Cyber resiliency delivery capability – LATAM |
| Benefits Achieved | Overall resiliency improvement<br>Ability to support the meeting of related regulations<br>Continuous understanding of cyber risk<br>Ability to spread cyber awareness through the organization<br>Reduction in the number of incidents<br>Ability to understand backup requirement<br>Ability to respond to threats<br>Strength of the partnership |

*Exhibit 2*

## 'Ability to meet client future requirements': Assessment criteria

| Assessment Category | Assessment Criteria |
|---|---|
| Level of Investments | Investment in Consultancy Services |
| | Investment in Business Continuity Planning |
| | Investment in Cyber related legal consulting |
| | Investment in Compliance consultancy and management services |
| | Investment in Managed security for networks/infrastructure |
| | Investment in Application security services |
| | Investment in Digital identity services |
| | Investment in Incident response services |
| | Investment in Backup and recovery services |
| | Investment into scoring risk |
| | Investment into AI/ML to support cyber resiliency operations |

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