NEAT EVALUATION FOR DXC TECHNOLOGY:

Cyber Resiliency Services

Market Segment: Overall

Introduction

This is a custom report for DXC Technology (DXC) presenting the findings of the 2024 NelsonHall NEAT vendor evaluation for *Cyber Resiliency Services* in the *Overall* market segment. It contains the NEAT graph of vendor performance, a summary vendor analysis of DXC for cyber resiliency services, and the latest market analysis summary.

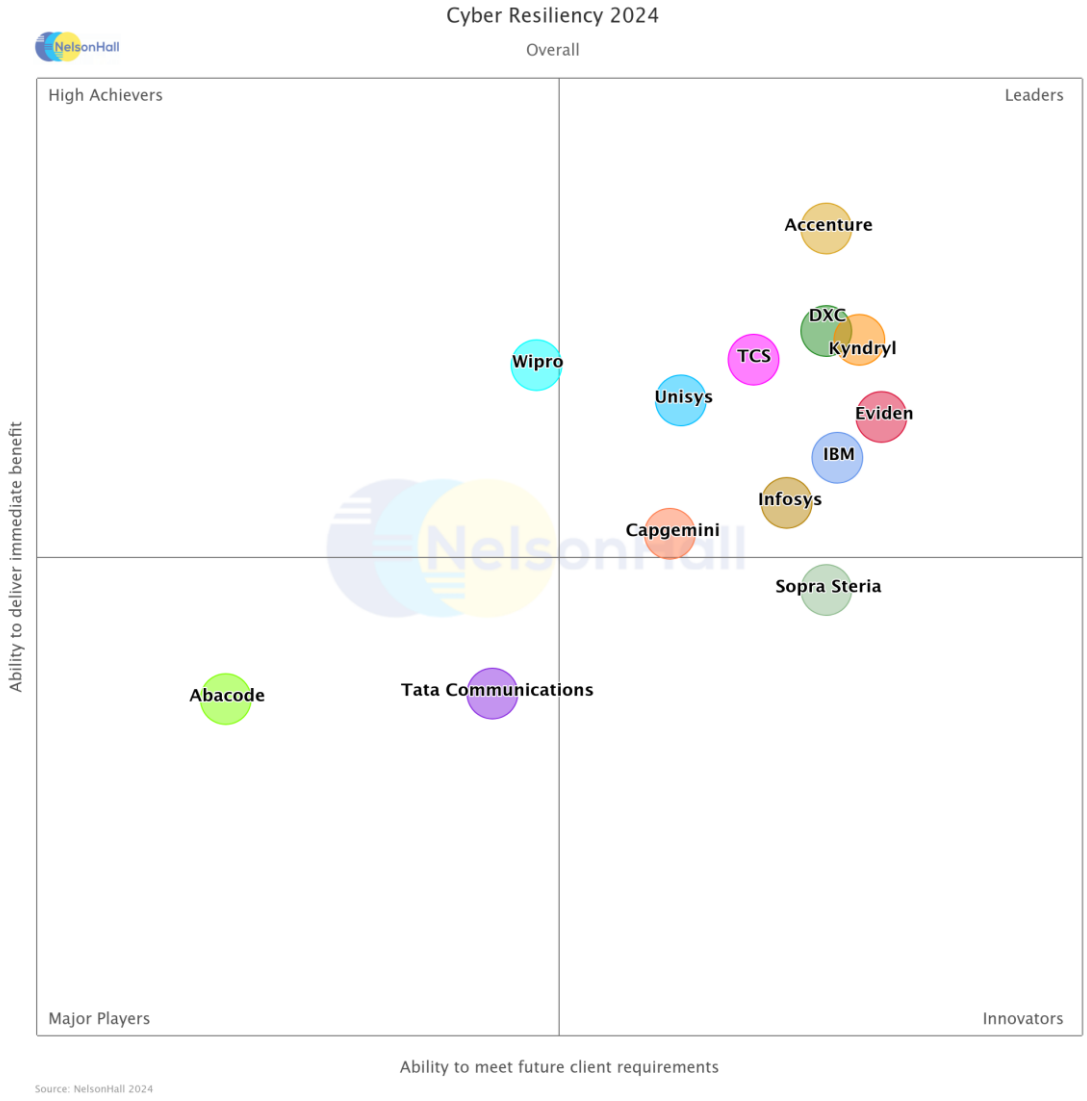
This NelsonHall Vendor Evaluation & Assessment Tool (NEAT) analyzes the performance of vendors offering cyber resiliency services. The NEAT tool allows strategic sourcing managers to assess the capability of vendors across a range of criteria and business situations and identify the best performing vendors 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 DXC as a Leader in the *Overall* market segment, as shown in the NEAT graph. This market segment reflects DXC'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.

Vendor Analysis Summary for DXC

Overview

DXC offers end-to-end security services, from advisory to architecture, implementation, and management. DXC's approach aims to protect, detect, and secure clients' operations throughout digital transformations. Security services include advisory services and managed security services for:

- Cyber risk and compliance management
- Digital identity
- Cyber transformation and operations
- Infrastructure, application, and data protection
- Data backup and disaster recovery.

These services are supported by the company's Cyber Reference Architecture (CRA), an independent set of tools and technologies that captures best practices from DXC's prior work with clients and Cyber Maturity Review (CMR).

New cyber resiliency services offered by DXC include:

- Partnership with Amazon for the use of its Amazon Security Lake, which provides a data lake for security events and supports analytics/AI/ML capabilities to detect cyber events in the data
- Services in support of Microsoft Entra, offering pre- and post-sales and consumption driven workshops. DXC will continue to develop the Entra program as clients seek to rationalize license costs during identity modernization activities
- External Attack Surface Management, for which DXC leverages its partnership with CyCognito for the use of its ASM platform. Using CyCognito, DXC maps the organization and discovers assets, prioritizing which ones are important, and identifies security gaps in these important assets to be remediated.

Financials

NelsonHall estimates DXC's H1 CY23 resiliency revenues to be $300m, with the following estimated breakdown by service:

- Cyber consulting services: $5m
- Managed cyber resiliency services: $125m
- Cyber compliance services: $50m
- Incident response services: $25m
- Backup and recovery services: $20m
- Application security services: $60m
- Cyber software and solutions: $15m.

Strengths

- DXC's ability to offer cybersecurity as part of an end-to-end IT service capability benefits clients as this allows them to experience a holistic service; with DXC being familiar with the client's business, it is better able to respond to threats and build business continuity plans. DXC is now boosting this capability through initiatives to force greater collaboration between the wider DXC services teams and security
- DXC uses one of the most extensive security research capabilities to develop detailed blueprints and work packages in its CRA. This enables DXC to provide clients with quick implementations and estimations of service
- Large client examples within vehicle security and VSOC, which is an increasingly important area of security as regulations take effect in the coming years
- Strong Microsoft security practice with client use cases that demonstrate the ability to implement Sentinel, to connect a large number of log sources without interruption, and to connect Entra to a large number of applications
- Extremely wide network of cybersecurity, disaster recovery, and cyber forensic centers and staff.

Challenges

- Competitors already launching software bill of materials services to increase ongoing application security monitoring capabilities
- DXC needs to continue its investment in GenAI to bring value to its customers in a fast evolving market where its competitors are attempting to do the same
- Clients are more open to multi-sourcing and are less likely to opt for an all-in-one service from an end-to-end provider offering security in support of an IT services contract such as DXC
- Competition from the consultancies for services benefiting from third-party arbiters such as auditing and consultancy for legal/compliance. The consultancies are currently in the process of building out managed security services capabilities. Although this lacks in-depth knowledge of the client's operations from an IT service capability, both have industry knowledge.

Strategic Direction

DXC primarily sells its cyber resiliency services across the wider DXC portfolio, for example embedding cloud security services into its infrastructure services and application security as part of shifting left into DevSecOps. Additionally, DXC is supporting clients that did not initially opt for DXC security services by responding to cyber security incidents with best practices for recovery, following up with tabletop exercises and breach preparation services.

A major go-to-market opportunity for DXC has been supporting clients that seek to consolidate and update their cyber resiliency tools.

Services that DXC is currently investing in include:

- Developing services on the Amazon Security Lake for which DXC announced an acceleration of its partnership with Amazon on AWS security
- Building application security services related to the software bill of materials
- Continuing to expand the Microsoft security practice. DXC has started working with clients on the use of Microsoft Copilot for security and is currently researching how the company can add value to clients by contextualizing information from Copilot by adding vertical, geographic, and regulatory information
- Within the digital identity space, DXC is investing in customer identity and access management (CIAM), Cloud infrastructure entitlement management (CIEM), SaaS migrations for CyberArk and SailPoint, Microsoft Entra, and passwordless authentication
- Bringing GenAI into its cyber resiliency services with partner AI capabilities, building platform and services capability in support of GenAI, and supporting clients in managing security challenges that come with implementing GenAI.

Outlook

DXC has consistently been a strong player in the cyber resiliency space, supported by its extensive research capabilities and blueprints, playbooks, and security platforms which offer robust management of clients' cyber profiles.

While DXC has been at the forefront of bringing to market next-generation services at an enterprise scale over this timeframe, NelsonHall would like to see more investment across the portfolio in the likes of automation and SBOM for which the competition is currently launching improved services. In these next-generation services, DXC needs to continue to find its value-add to increasingly intelligent platforms by adding contextual information and best practices from its security frameworks.

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 Business Continuity Planning Cyber related legal consulting Compliance consultancy and management services Managed security for networks/infrastructure Application security services Digital identity services Incident response services Backup and recovery services
Delivery Capability	Use of security accelerators Ability to reevaluate resiliency at regular intervals Application of AI/ML to reduce risks, support cybersecurity employees, and respond to threats 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 resiliency improvement Ability to support the meeting of related regulations Continuous understanding of cyber risk Ability to spread cyber awareness through the organization Reduction in the number of incidents Ability to understand backup requirement Ability to respond to threats 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