NEAT EVALUATION FOR UNISYS:

Cyber Resiliency Services

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

Introduction

This is a custom report for Unisys presenting the findings of the 2024 NelsonHall NEAT vendor evaluation for *Cyber Resiliency Services* in the *Overall, Incident Response & Backup Services,* and *Managed Cyber Security Services* market segments. It contains the NEAT graphs of vendor performance, a summary vendor analysis of Unisys 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.
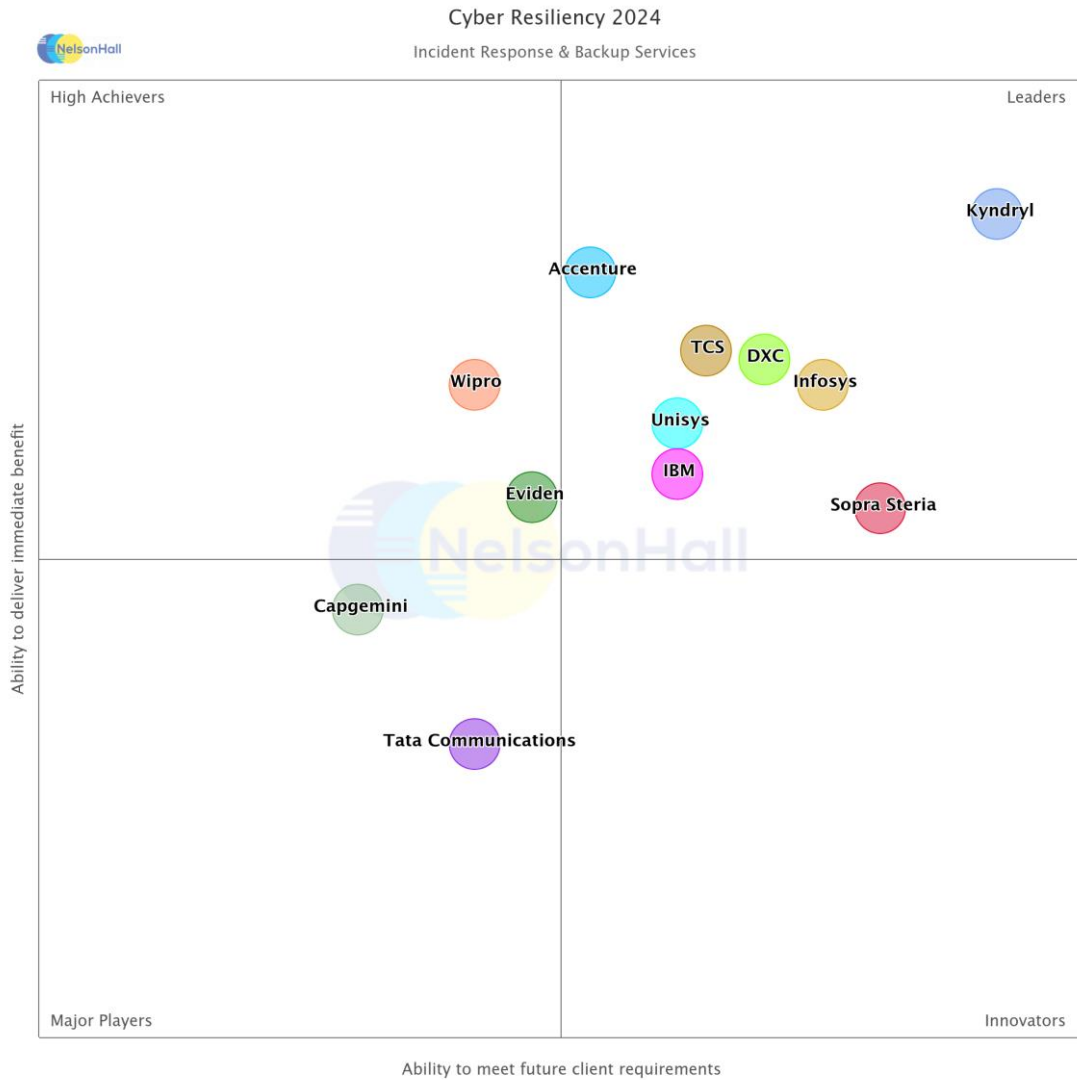
NEAT Evaluation: Cyber Resiliency Services (Overall)
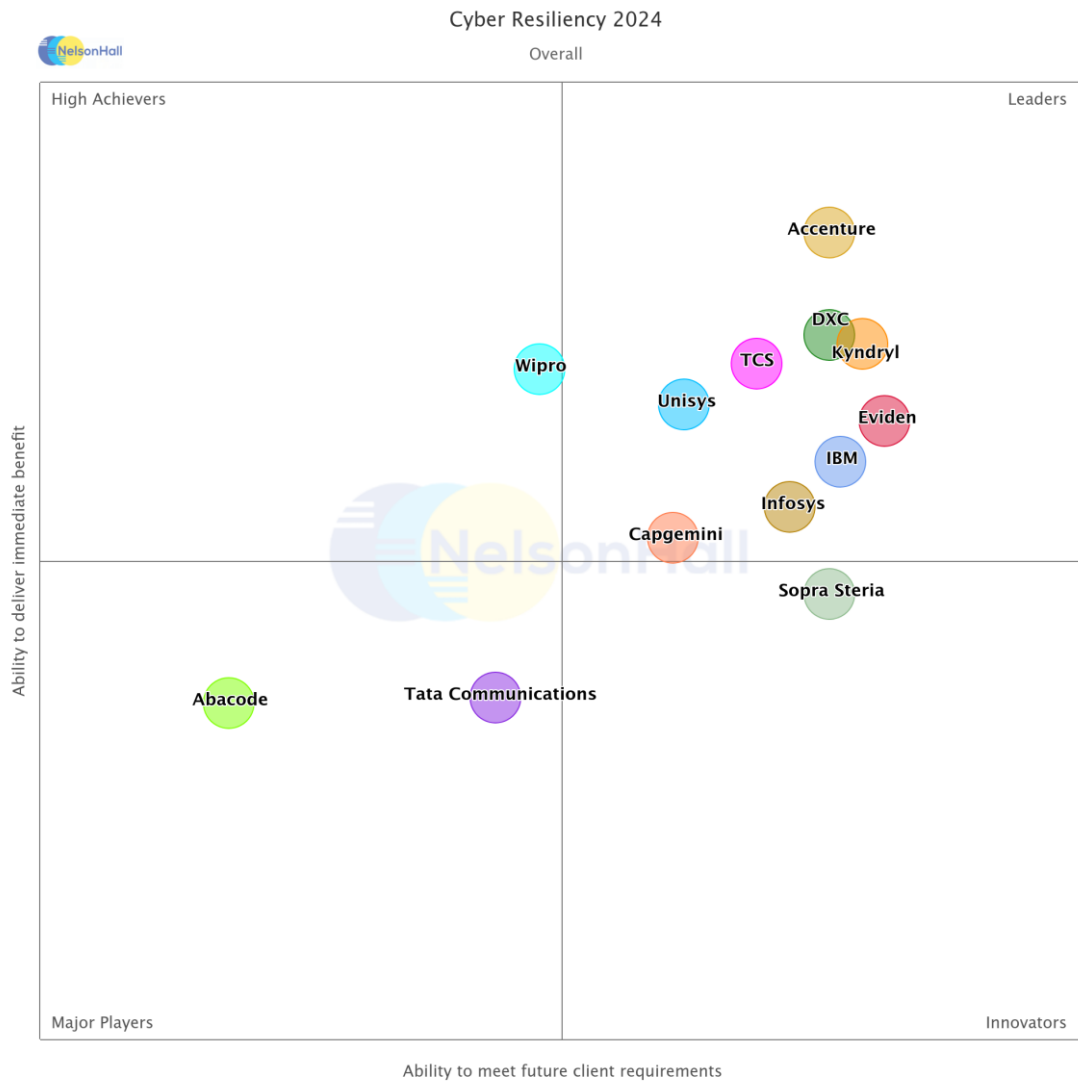
NelsonHall has identified Unisys as a Leader in the *Overall* market segment, as shown in the NEAT graph. This market segment reflects Unisys' overall ability to meet future client requirements as well as deliver immediate benefits to its cyber resiliency clients.

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 (Incident Response & Backup Services)
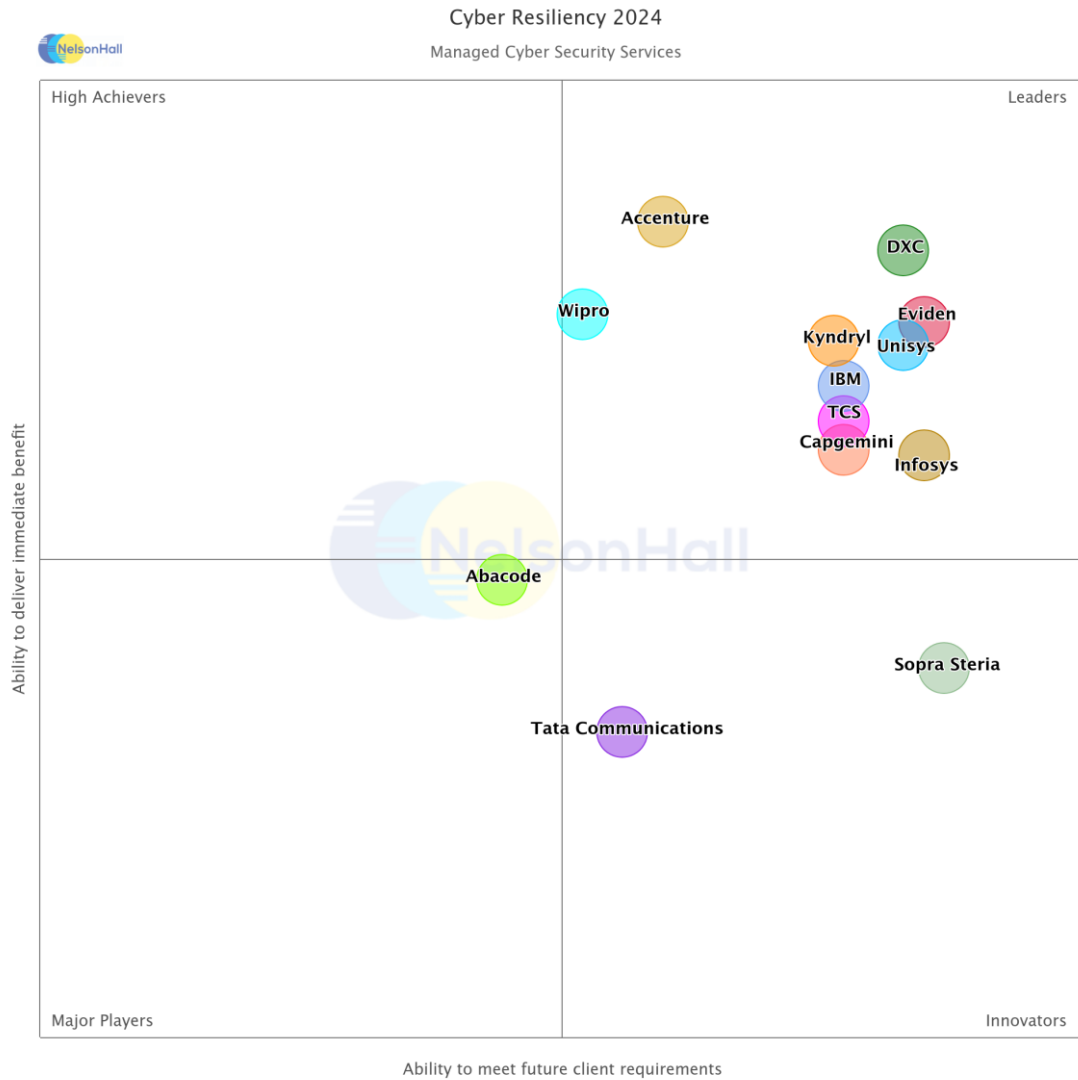

NelsonHall has identified Unisys as a Leader in the *Incident Response & Backup Services* market segment, as shown in the NEAT graph. This market segment reflects Unisys' ability to meet future client requirements as well as deliver immediate benefits to its cyber resiliency clients with specific capability 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)

Cyber Resiliency 2024
Managed Cyber Security Services

NelsonHall has identified Unisys as a Leader in the *Managed Cyber Security Services* market segment, as shown in the NEAT graph. This market segment reflects Unisys' ability to meet future client requirements as well as deliver 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 Unisys

Overview

Unisys' cyber resiliency services consist of:

- Cybersecurity consulting
- Implementation services
- Managed security.

In supporting clients in assessing risk tolerances, Unisys uses its assessment and solution capabilities suite to assist client's define a tailored security resilience business case.

This suite includes NIST aligned maturity assessment, domain assessments including cyber resilience, and client sourcing security governance joint responsibility assessments, that ingest security data to analyze the client's cyber risk posture break down the possible scenarios that could affect the client with details on risk posture, threat likelihood, business impact, control effectiveness, cyber peril probability, impact, and expected loss.

Unisys' Attack Surface Discovery solution provides assessment vulnerability exposure insights as well as ongoing attack surface management services for clients' evolving internet attack surface. The Attack Surface Discovery solution requires no installation, is transparent, and silent to a client's cyber defense systems; rather, the clients provide entity names to be investigated from which Unisys can provide initial insights, such as discoverable assets, various vulnerabilities and exposures, as well as PII dark web leakage within 15 days.

Unisys' managed XDR solution builds on an innovative vendor ecosystem including LogRhythm, Securonix, MS Sentinel, and HumanSecurity to deliver client tailored and vertically integrated security observability and response solutions.

Unisys adds advanced analytics into its solution. These advanced analytics include:

- Malware behavioral risk – to provide ranked and scored endpoints exhibiting malware-like behavior
- Reconnaissance behavior – to rank the risk that endpoint is engaged in mapping internal networks
- Dark web correlation – events correlated with targeted activity
- Malicious insider risk – risk that a human insider is engaged in malicious activities
- Long-time frame malicious behavior – to detect low and slow attacks.

Unisys Secure Segmented Network Access solution offers clients a suite of capabilities across their network zero-trust roadmap, providing client tailored network security solutions for MPLS, SD-Wan, SASE, and full zero trust networks.

Unisys' Security Device Management (SDM) offerings aim to effectively manage and maintain security devices remotely in an enterprise. Unisys has an ecosystem of partners including Lookout, Palo Alto, and Fortinet, and maintains its own proprietary Stealth Core product for advanced micro-segmentation capabilities to deliver client tailored network security and response solutions.

Stealth is Unisys' micro-segmentation security software, which allows users to create identity-focused communities of interest. Users and devices outside these communities cannot

intercept network traffic or understand the data between community members, so critical assets and data are hidden from adversaries.

Unisys has expanded its cyber recovery and resilience capabilities, utilizing partnerships including. Rubrik, and SecuritySnares.

Financials

Unisys' H1 2023 revenues were $993m, up 3.3% y/y. Revenue by business unit was:

- Cloud, Application & Infrastructure Solutions (CA&I), in which the majority of cyber resiliency business resides (alongside hybrid and multi-cloud management, application modernization, cloud-native application development, and data analytics and insights) – $259m, down 0.2% y/y

- Digital Workplace Solutions (DWS) – $266m, up 5.6% y/y

- Enterprise Computing Solutions (ECS) – $323m, up 5.4% y/y

- Other – $146m, up 1.2% y/y.

NelsonHall estimates Unisys' H1 2023 cyber resiliency revenues to be $155m.

Strengths

Rather than protecting against threats across a client's network, Unisys' Stealth offerings protect important data by effectively masking it and its transfer undetectable; no other offering provides this level of obscuring network topology from potential attackers. The Stealth suite has been accredited by the NIAP and has been integrated into partner technologies.

Challenges

- Following the sale of the federal business to SAIC, the R&D for new services and platform capabilities within the cybersecurity unit has slowed down. Likewise, the company's mindshare within cybersecurity has declined.

Outlook

Unisys' cyber resiliency services are built around five core domains; continuous threat exposure management, extended detection and response, digital identity and access management, secure segmented network access, and cyber recovery and resilience. The company is actively expanding its partner innovation ecosystem underpinning a strategy for tailored and integrated secure business solutions, based on reference architectures and vendors, co-creating with client's prior cyber defense initiatives and investments

Unisys has, however, fallen behind in its R&D efforts with no major releases of the Stealth platform or other similarly important IP, and less attempts to retain its mindshare in cybersecurity.

The company is one of the most experienced vendors in providing NIST-certified FAIR risk assessments. This allows the company to better support a client in selectively building its cyber resiliency posture and prioritizing risks effectively.

NelsonHall would like to see the release of more services such as continuous compliance and security for, and using, GenAI solutions.

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.