

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 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 for cyber resiliency services.

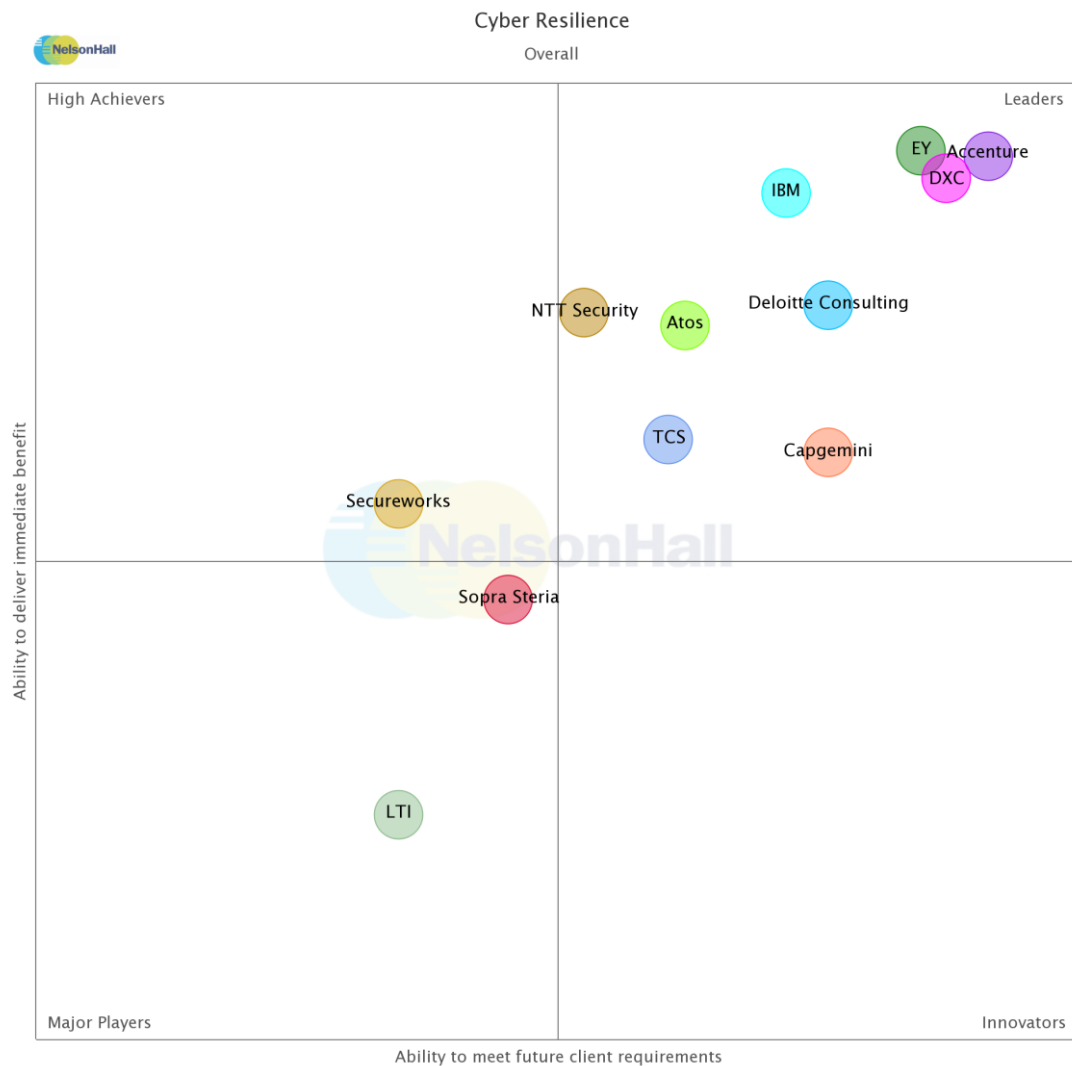
This NelsonHall Vendor Evaluation & Assessment Tool (NEAT) analyzes the performance of vendors offering cyber resiliency services. The NEAT tool allows strategic sourcing managers to assess the capability of vendors across a range of criteria and business situations and identify the best performing vendors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

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

Vendors evaluated for this NEAT are: Accenture, Atos, Capgemini, Deloitte Consulting, DXC Technology, EY, IBM, LTI, NTT Security, Secureworks, and Sopra Steria, and TCS.

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 cyber resiliency services clients.

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

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

Vendor Analysis Summary for DXC Technology

Overview

DXC's cybersecurity services reside within its infrastructure technology service business with its cloud, workload platforms, and its workplace, mobility and security solutions. Security is also one of the components of DXC's digital business (~17% of revenues) along with cloud apps, consulting, analytics, and cloud infrastructure.

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

- Security risk management
- Intelligent security operations
- Identity and Access Management (IAM)
- Infrastructure and endpoint security
- Data protection and privacy.

Advisory services include risk management, including DXC's security diagnostics services leveraging Cyber Maturity Reviews (CMRs): 'foundation,' 'full,' 'GDPR deep dive', and 'ransomware deep dive'. The CMR consists of structured reports around 24 capabilities, what technical security controls the client has, and how they are managed vs. strategic and regulatory requirements.

Managed security services include DXC's intelligent security operations that monitor the client's environments and reduce the complexity of securing the IT environment. DXC's threat intelligence platform is being designed to be increasingly modular, collecting security information from a number of different sources including ArcSight, which currently is the leading log collection platform, into a Hadoop data lake for analysis.

DXC operates two tiers of 24x7x365 security operations center: global security operations centers and regional security operations centers. Its global security operations centers (GSOs) are based in:

- U.S. – Plano, Texas and Newark, Delaware
- U.K. – Aldershot
- Australia – Sydney.

DXC's three forensic response centers are co-located in SOCs in the U.S., U.K., and Bulgaria. DXC has ~3.5k security and compliance FTEs.



Financials

NelsonHall estimates DXC's CY18 revenue to be \$21.8bn. Within its Global Infrastructure Services (GIS) line which includes enterprise cloud apps, consulting, security, analytics, and cloud, revenue was ~\$12.2bn. NelsonHall also estimates that DXC resiliency revenues to be \$880m up ~8%, with the following estimated breakdown, by geography:

- Americas: 50% (~\$440m)
- EMEA: 45% (~\$410m)
- APAC: 5% (~\$50m).

Strengths

- The ability to offer cybersecurity as part of an end-to-end IT services capability; as part of this capability, DXC has a greater ability to know the client's business and can better respond to threats and build plans for business continuity
- One of the largest security research capabilities used to develop detailed blueprints and work packages in its CRA to enable DXC to provide clients with quick implementations and estimations of service
- DXC has a large scale in cybersecurity, demonstrated by its global network of SOCs and 4k cybersecurity FTEs that can support the majority of large-scale security contracts.

Challenges

- Clients are more open to multi-sourcing and less likely to opt for an all-in-one service from an end-to-end security provider or provider that offers security in support of an IT services contract, such as DXC
- Competition from lower price MSSPs expanding service offerings into more advanced security services
- 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 progress of building out MSS capabilities, and although this lacks as deep a knowledge of the client's operations from an IT services capability, each has industry knowledge.

Strategic Direction

Following two years of portfolio rationalization following the merger of HPE and CSC's security units, DXC security has produced a roadmap for 2020-2022 that includes:

- Further integration into the 'platform DXC' and Bionix initiatives. Through further integration into platform DXC, DXC will be able to further leverage automation across services provided for clients, i.e. providing more automated response services with DXC Bionix
- Further focus of cloud and IoT/OT first across industries, then focusing on industry-specific offerings (see below)



- A deeper alignment to industry sectors through the build of industry-specific points of view and industry-specific blueprints, playbooks, and offerings. Target verticals for the build of industry-specific IoT offerings include manufacturing, energy and utilities, healthcare, and transportation
- As part of the strategy, DXC will look to integrate more AI into security services, to continue the use of AI for analytics and towards the end of the period, investing in services for the security of AI systems.

Outlook

DXC has extensive cybersecurity research capabilities, numerous blueprints and playbooks such as the CRA to enable DXC to protect client environments quickly and more fully.

DXC aims to provide resiliency as part of a wider IT services engagement for which it would have a deeper knowledge of client business operations and be more able to support large enterprises in becoming and remaining resilient.

As DXC invests in more advanced security services and focuses on the likes of AI, IoT, and bots, it will introduce more services to cater to these offerings, and as such will be focusing more on industry-specific offerings.

Cyber Resiliency Services Market Summary

Buy-Side Dynamics

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

- Organizations traditionally separating cybersecurity from business operations, with CISOs often struggling to present business cases and ROI for cybersecurity and build responses into BCM plans
- An increasing number of applicable regulations for organizations to meet, including those set from regions other than the organization's operational location. These are too often seen as the standard level of defense, despite lagging behind new technologies such as IoT and blockchain
- Organizations having a large number of legacy applications that require investment to patch. Organizations may find this patching process uneconomical weighed against the risk of being attacked
- Cybersecurity talent continues to be incredibly hard to hire, even more so for candidates with a business background who can relate the issues of cybersecurity to the organization's operations
- Increased sophistication of attacks, with hackers using exploits developed by state-sponsored organizations that further their spread or make recognizing spoofing more difficult
- An increasing amount of data being collected on customers which, should they be breached, can damage the organization's reputation
- The often-overlooked human factor of cybersecurity: users are unaware of what IoCs look like and how to react to an IoC.

Market Size & Growth

The current global resiliency services market size is estimated by NelsonHall at ~\$22.5bn and will grow to ~\$49bn by 2023, a CAGR of 16.8%.

Growth will be driven by:

- Clients building resiliency into other operations, i.e. DevSecOps
- Regulations increasing minimum standards
- New technologies such as IoT, blockchain, and later, quantum computing.

North America accounts for 44% of the cyber resiliency market, and is the most mature region. Growth in North America is being driven by clients adopting services to add cybersecurity into BCM plans.

APAC cyber resiliency is generally less mature than in its Western counterparts. A growth driver in APAC will be the high use of IoT technologies.

Success Factors

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

- Security brought into client discussions early
- Close ties between IT services, business operations, and cybersecurity
- Use of ML/AI tools to detect and reduce the MTTD and MTTR of threats, and reduce the requirement to have as many L1/L2 security analysts investigating events
- Industry expertise in both the threat database and in the consulting and management of resiliency to truly understand industry best practices, in addition to the typical threats and regulations to which the client is subject
- Being able to look beyond the role of the employee to assess the minimal access required to operate as part of insider protection/data segmentation
- Understanding the client business and the security market enough to provide ROIs on integrating a security tool/provide a service
- Developing delivery capabilities in support of onshore delivery should the contract require it for regulatory purposes (e.g. mission critical infrastructure)
- Positioning as a thought leader in resiliency with strong connections with the C-level and with nation states/regulatory bodies.

Outlook

Over the next few years:

- Security strategies will be developed alongside business operations and BCM plans, as organizations deal with the use of technologies such as IoT
- Training will be developed and deployed across organizations to which users respond positively and view it less as a box ticking exercise; self-service reference guides and checking facilities will be deployed in organizations
- ML and AI will practically eliminate L1/L2 SIEM services, and the development of new technologies will enable detection of unusual network activities
- Security testing activities to become further divided across automated efforts with security tools, and with advanced manual red team testing that examines the likes of physical security
- Application security is to be baked into ADM activities as vendors mature DevSecOps activities
- Advanced ML technologies that replace or support typical role-based access management and further use of IoT to manage access by location
- Further regulations to be developed at the region and industry level for which vendors will develop further technologies for automatically detecting changes in the client's operation that breach regulations
- Cloud providers to continue to develop security technologies as a differentiator, with vendors providing management of these in-built security tools



- Further development of tools and technologies, and changes in client attitudes to automated remediation of security events
- Cybersecurity will be truly valued in BCM setups and involve security early in the establishment of BCM plans. Incident response plans in general to consider the reputational damage of an event.



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

*Exhibit 1***‘Ability to deliver immediate benefit’: Assessment criteria**

Assessment Category	Assessment Criteria
Offerings	<ul style="list-style-type: none"> Simulation or espionage services Cyber resiliency strategy development Legal consultancy services for cybersecurity Penetration testing SIEM Application security Endpoint and edge security Identity management services Security compliance services Incident response services- Backup and recovery services Level of automation/cognitive security capabilities
Delivery	<ul style="list-style-type: none"> Delivery in support of U.S. Delivery in support of U.K. Delivery in support of Rest of EMEA Delivery in support of APAC Delivery in support of LATAM Onsite support of MSS Language support Scale of FTE support Security IP Single touch point
Presence	<ul style="list-style-type: none"> Financial services security presence Government security presence Manufacturing security presence Retail security presence Energy & utilities security presence
Benefits Achieved	<ul style="list-style-type: none"> Detection and response time Response to cyber threats Value for money Threat avoidance Ability to remain in compliance with regulation Improved visibility through dashboard or portal Improved staff knowledge

*Exhibit 2***‘Ability to meet client future requirements’: Assessment criteria**

Assessment Category	Assessment Criteria
Future Offerings & Delivery	Area of investment in centers: onshore
	Area of investment in centers: offshore
	Investment into cyber consultancy services including simulation and espionage services
	Investment into legal consultancy services for cybersecurity
	Investment into network security
	Investment into application security
	Investment into advanced security services
	Investment into backup and recovery services
	Investment in automation/cognitive security capabilities
Commitment to Cyber Resiliency	Investment into security dashboards
	Outlook for revenue expansion
	Strength of partnership
	Likelihood of recommending

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



research.nelson-hall.com

Sales Enquiries

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

Simon Rodd at simon.rodd@nelson-hall.com

Important Notice

Copyright © 2019 by NelsonHall. All rights reserved. NelsonHall exercises its best efforts in preparation of the information provided in this report and believes the information contained herein to be accurate. However, NelsonHall shall have no liability for any loss or expense that may result from incompleteness or inaccuracy of the information provided.