NEAT EVALUATION FOR CAPGEMINI:

Managed Security Services

Market Segment: Overall

This report presents Capgemini with a customized summary of the 2017 NelsonHall NEAT vendor evaluation for Managed Security Services (MSS). It contains a summary vendor analysis of Capgemini in MSS, and the latest market analysis summary for MSS. An explanation of the NEAT methodology is included at the end of the report.

The vendors evaluated for this NEAT evaluation are Atos, CGI, Capgemini, CSS Corp, DXC Technology, IBM, Infosys, SecureWorks, TCS, and Unisys.

Introduction

NelsonHall has assessed and evaluated Capgemini's proposition against demand for Managed Security Services (MSS), and has identified Capgemini as a Leader in the *Overall* market segment. The *Overall* market segment reflects vendors' overall ability to meet future client requirements as well as delivering immediate benefits to MSS clients.

Mike Smart, Senior IT Services Analyst with NelsonHall, said, "Capgemini was identified as a leader in the MSS NEAT evaluation due to its investment in security, from the establishment of its cybersecurity global service line, to new reusable services, and expansion of cybersecurity delivery. The use of its 'right people, right process with the right toolset' model is demonstrated through its robust cybersecurity academy, its recently launched multi-tenant managed SOC and threat hunting service offerings, and its big data partnership with Pivotal, which is being applied to anomalous behavior detection."

Buy-side organizations can access the MSS NEAT tool *here*.

MSS Vendor Analysis Summary for Capgemini

Overview

Capgemini offers a range of cybersecurity services including:

- Strategy, governance, and people security consultancy services:
  - Digital security assessment, strategy and risk management
  - Cybersecurity awareness and training
- Transformation cybersecurity implementation:
  - Security transformation and operating model implementation
  - Program management, change and communication management
- Build and operations cybersecurity testing and running operations:
  - Application security testing and technical security testing
  - Implementation of security solutions and managed security services.

Within its security practice, Capgemini has 3k FTEs including 600 dedicated FTEs operating from its networks of dedicated client SOCs, multi-client SOCs, and multi-tenant SOCs.

Capgemini uses a mix of ~10 dedicated client SOCs, five multi-client SOCs, and two multi-tenant managed SOCs.

Multi-client SOCs are located in:

- Toulouse, France
- Luxembourg
- Inverness, Scotland
- Brussels, Belgium
- Asturias, Spain
- Bangalore, India
- Mumbai, India.

Financials

NelsonHall estimates Capgemini's CY16 revenues to be ~€12.4bn. Of this, it estimates Capgemini's CY16 total cybersecurity revenues at €270m, of which:

- Application security testing: ~€20m
- Security consulting: ~€100m
- Managed security services: ~€150m.

Strengths

- Willingness and proven ability to establish dedicated SOCs to take over the management of clients' security
- High levels of investment demonstrated through the establishment of the GSL, the investment in SOCs, new reusable services, and expanding the cybersecurity partner network
- Having a high European presence, Capgemini should benefit from the introduction of regulations such as GDPR (to be introduced in May 2018), forcing clients to meet compliance, and will use this as a springboard to gain extra MSS clients
- Strong experience in SCADA security, with capabilities added through the acquisition of Euriware
- Strong partnership with Pivotal on big data analytics, which is being applied to anomalous behavior detection.

Challenges

- Late in making cybersecurity a top priority, and developing and marketing a strong set of cybersecurity offerings
- One of Capgemini's growth strategies for cybersecurity revolves around clients that are unaware of their security responsibilities in moving to the cloud. Capgemini was relatively late into the cloud infrastructure migration and management space, formally bundling its Cloud Choice offering in 2015. While its cloud engagements may support growth in cybersecurity, Capgemini has not currently made the same progress in its cloud offerings as several competitors to support this growth.

Strategic Direction

Capgemini employs a 'right people, right process with the right toolset' model, along with its rightshore model, to deliver cybersecurity services. As part of this, it has developed its cybersecurity academy and graduate program which have resulted in an unusually high retention rate. To ensure that the right toolset is used, Capgemini reevaluates its technology partners every six months, and will continue to expand its partner network. As part of this partner network expansion, Capgemini will expand its threat intelligence network to launch a verticalized threat intelligence network.

Capgemini is targeting 50% growth in CY17; to achieve this growth it will continue to target clients that currently do not know their responsibilities on public, private and hybrid clouds. Capgemini is investing heavily in this consultancy capability, with new services to be introduced on Office 365.

Capgemini has been investing heavily in its SOCs; it is both building new SOCs and relaunching its current SOCs as third-generation multi-tenant managed SOCs. The third-generation SOC provides advanced data analysis to prevent APTs. Currently, Capgemini's Indian SOCs have been relaunched as third-generation SOCs, with plans to relaunch the Madrid SOC in CY17.

As part of the investment in its SOCs, Capgemini is expanding its footprint, and is looking both at North America (cross-selling to IGATE clients) and Asia Pacific in 2017.

Capgemini is also investing in automating security testing and is helping drive automated security testing in its HPE partnership. The advantages of automating testing include decreasing the time needed for testing, and allowing Capgemini to reallocate FTEs to advanced security research.

Capgemini will be adding a new threat hunting service in Q1 2017, with a lightweight agent to monitor persistent programs with high levels of malicious activity and modified legitimate programs. The agent used to monitor programs can be deployed within eight hours. The new service has been in beta testing with three clients.

Outlook

Capgemini's recently established security GSL focuses on building reusable services across countries targeting Hadoop security, software-defined datacenter security, and hybrid cloud security.

In 2017, expect high double-digit growth in the security GSL via expansion in the cybersecurity portfolio, with services such as threat hunting, geographic expansion (leveraging its IGATE acquisition), and inorganic growth in Asia Pacific in 2017 or 2018.

MSS Market Summary

Buy-Side Dynamics

Key challenges for organizations looking to outsource MSS:

- Increasing cost of cybersecurity, while demonstrating ROI
- Access to cybersecurity skills and up-to-date information
- Ability to respond quickly to threats
- Ability to gain a holistic view of cybersecurity
- Strengthening social engineering around security
- Uneven workloads.

Market Size & Growth

The current global MSS market size is estimated by NelsonHall at ~$9bn and is on target to reach ~$17.6bn by 2021, a growth of 12.2% CAGR.

Growth will be driven by:

- Regulatory pressure
- Responses to an increasing number and complexity of attacks
- The introduction of complementary services.

North America accounts for 43% of the MSS market. Vendors with American ties are slow to make progress in APAC. Vendors will continue to look for growth in APAC, firstly through supporting clients from Australia based SOCs, then with CoEs stationed in e.g. Singapore and Hong Kong.

Success Factors

Critical success factors for vendors within the MSS market are:

- Ability to develop a strong go-to-market that demonstrates vendor strengths in cybersecurity research/delivery
- Ability to have a strong level of cybersecurity research that analyzes past events to strengthen indicators of compromise and reduce the number of false positives and negatives
- Ability to keep abreast of upcoming changes in cybersecurity regulations. High-level vendors, working with the public sector, and industry alliances can influence these regulations
- The development of strong cybersecurity talent and recruitment programs. These programs partner with universities to hire graduates, and target white-hat hackers and previously untapped members of the talent pool, through diversification

- The development of security operations centers in regions to support specific clients. Vendors have additional FTEs in countries outside of SOCs to support languages other than English
- Ability to demonstrate the ROI of cybersecurity services. Vendors run wargame scenarios and vulnerability assessments to demonstrate how a cyber-attack can affect a client's operations
- For traditional ITS providers, the ability to involve cybersecurity teams for bid support on ITS contracts
- The ability to rationalize the services from acquired parties. For example, the acquisition of HPE ES by CSC (where HPE ES is the stronger party in terms of cybersecurity). The combined company, DXC Technology will benefit from the strong overlap in cybersecurity tools used by both parties, whatever the overlap in cybersecurity centers and services that require rationalization.

Outlook

Over the next few years:

- Regulations will come into force, e.g. GDPR in 2018, which will affect organizations with EU operations. These regulations will inform the introduction of cyber regulations in emerging markets
- Security threats that risk corporate reputation and regulations will force cybersecurity to be a hygiene factor
- Vendors to continue to restructure and relaunch cybersecurity portfolios around cloud security and to rationalize acquired offerings
- Vendors to focus branding of security offerings around securing clients' reputation
- As more robust, automated security tools are developed, the requirement for vendors to perform SIEM rule tuning reduces, allowing vendors and clients to focus on more advanced threats
- Vendors will embed true AI, machine learning, and automation into all their cybersecurity offerings to detect and respond to threats more quickly and accurately. A standout example of this is IBM investing in integrating Watson for cybersecurity. Vendors unable to add AI will partner with the typical tool providers
- The lack of effectiveness of typical encryption will require advanced encryption techniques to be built into technologies such as blockchain
- In 2020, revenue from threat management services such as cyber resiliency services will overtake security management to be 24% of the managed security market. Vendors that have partnered with cybersecurity insurers will see the most demand for cyber-resiliency services
- Technology supporting securing new developments such as IoT and full DNS record scanning will require new approaches of collecting, analyzing, and storing security data on a much larger scale. The use of quantum computing for security such as quantum cryptography should be assessed.

NEAT Evaluation for MSS: Methodology

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	SIEM Application security Endpoint security IAM Threat database maturity Penetration testing Ability to offer security as part of a larger ITS contract Insider protection IoT security services Level of automation Dashboard or portal offered
Delivery	Ability of offer dedicated delivery 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 Offshore focus for shared service MSS Onshore focus for shared service MSS Onsite support of MSS Language support Scale of FTE support Security IP Single touch point
Presence	Financial services security presence Government security presence Manufacturing security presence Retail security presence Energy & utilities security presence
Benefits Achieved	Detection and response time Cost reduction Threat avoidance Improved visibility through dashboard or portal

Exhibit 2

'Ability to meet client future requirements': Assessment criteria

Assessment Category	Assessment Criteria
Investment in Cybersecurity	Area of investment in centers: onshore Area of investment in centers: offshore Investment into security dashboards Investment in automation Investment in threat database Investment into advanced cybersecurity services Investment into IoT security Investment into insider protection and physical security Investment into network security Investment into application security
Commitment to MSS	Industry specific security research Security FTE growth Financial rating Likelihood to partner for security services

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:

Guy Saunders at guy.saunders@nelson-hall.com

Important Notice

The information provided in this report shall be used only by the employees of and within the current corporate structure of NelsonHall's clients, and will not be disclosed to any other organization or person including parent, subsidiary, or affiliated organization without prior written consent of NelsonHall. 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.