VENDOR PROFILE

TCS, More Than a Trusted IT Services Provider – A Perspective on Its Enterprise Security and Risk Management Practice

Cathy Huang  Sherrel Roche

IDC OPINION

Technology buyers continuously rank security as their top concern when outsourcing, whether using traditional IT delivery methods or cloud-based options. The security concern is also greatly amplified when an enterprise undertakes a digital transformation (DX) journey and adopts new technologies such as internet of things (IoT), cognitive systems, and so forth. Tata Consultancy Services (TCS), a leading global IT services provider, has a proven track record of 18 years of building security solutions for its global customers. It also holds over 25 patents and intellectual properties (IPs) in security domain.

In recent years, TCS has consolidated all its security service capabilities under one unit called Enterprise Security and Risk Management (ESRM). This unit has rapidly expanded its security services and has now over 3,000 professionals worldwide. These combined capabilities help TCS manage the requirements of its 150 unique customers globally across consulting, systems integration, and managed services.

The vendor possesses a comprehensive portfolio of services in consulting, professional services, and managed services across all domains in cybersecurity, namely, network security, security operations, identity and access management (IAM), enterprise vulnerability management (EVM), privacy and data protection, governance, risk, and compliance (GRC), fraud management, digital forensics, cloud security, and mobile security. IDC believes TCS’ security business generated more than US$300 million in revenue in 2015 with revenue split across various verticals.

IN THIS VENDOR PROFILE

This IDC Vendor Profile analyzes TCS’ ESRM offerings, including managed security services (MSS), IAM, GRC services, security integration, and consulting services. This profile document describes the company’s current services offerings and assesses the key success factors — including company strategy, product strategy, offerings, partnerships, business strategy, and opportunities — for TCS’ security services offerings.

SITUATION OVERVIEW

Company Overview

TCS is a leading IT services player in the global IT services, digital, and business solutions market. The vendor has an integrated services portfolio across various domains, including application development and maintenance, IT infrastructure services, business process services, consulting, and ESRM. TCS offers customers a consulting-led end-to-end portfolio of IT and IT-enabled services delivered through its unique Global Network Delivery Model (GNDM), a globally recognized benchmark of excellence in software development.
The security portfolio of TCS has been growing over the last 18 years and now services more than 150 customers globally and drives over US$300 million (FY15) in revenue. TCS operates across multiple geographies and has over 3,000 professionals dedicated to security services worldwide. TCS manages 34 dedicated global security operation centers (SOCs) and 5 security centers of excellence (COEs). TCS also leverages its multitenanted shared SOCs to offer round-the-clock monitoring, threat intelligence, and incident response services. The vendor also employs a design, build, operate, and transfer model for customer-owned SOCs.

**Company Strategy**

**Product Strategy**

TCS offers security services based on its core capabilities — consulting, managed services, and systems integration across its ESRM portfolio. Its end-to-end security solutions consist of five mature practices and three fast-emerging practices. They are:

- **Established security services:**
  - **Managed security services.** TCS offers end-to-end yet customizable MSS programs from design and build to manage the security operation for the customers. At the same time, it also deploys a security incident and event management (SIEM) or an MSS portal access to the customer’s requirement.
  - **Identity and access management.** TCS' IAM services enable clients to assess their IAM maturity, define IAM strategy, and formulate the road map. IAM professional services cover identity management and governance as well as federation of various authentication, authorization, and role management solutions. In addition, TCS provides managed support services such as technical support, product upgrades, and maintenance implementations.
  - **Enterprise vulnerability management.** TCS' EVM services enable organizations to eliminate the intrinsic security weaknesses in web and mobile applications, network devices, and infrastructure by rigorous testing and review services. Banking on its strong expertise in the application management and testing domains, IDC believes TCS has a differentiated approach in handling vulnerability management within the complex application life-cycle management.
  - **Governance, risk, and compliance.** TCS' GRC services help enterprises manage the regulatory and compliance requirements, enable enterprises to identify risks, and take well-informed decisions to mitigate risks. Organizations gain in-depth insights into all aspects of GRC activities through automated tools in addition to assessing, evaluating, and treating their enterprise risks through the operational risk management framework. Based on the insights into risks, TCS assists organizations' designs and implements the necessary controls to manage the current regulatory and compliance requirements.
  - **Fraud management and digital forensics.** These services cover proactive fraud detection, investigation, prevention, digital forensics, and end-to-end ediscovery process management.

- **Fast-emerging security services:**
  - **Cloud security.** This service is often used when customers decide to adopt public cloud services or software-as-a-service (SaaS) solutions. TCS security professionals help clients plan a secure cloud migration road map and implement or leverage TCS' cloud security policy and framework and, more importantly, set up data protection and privacy for cloud.
- **Mobile security.** This is an extension of TCS security and risk management offerings to the enterprise mobile platform as well as mobile applications. It includes mobility strategy and policy formulation services, regulatory impact assessment, and mobile application threat modelling and code reviews.

- **Privacy and data protection.** TCS provides services around data security and privacy-enhancing tools (PETs) design and implementation.

In addition, TCS provides a structured cyber-resilience framework to guide clients through their varying cybersecurity posture. This framework is also very much in line with TCS' security strategy objectives, which is being the trusted security services partner for its clients and being able to offer a full suite of cybersecurity services across protect, detect, respond, and recover functions.

**Business Strategy**

TCS has taken a consulting-led approach for its comprehensive security services portfolio. Although TCS services clients globally, North America is the biggest client base for TCS, with majority of the revenues generated being from that region, followed by Europe. In Asia/Pacific, TCS has a good presence in Japan, Australia, and Singapore. TCS has clients across different industries, with banking, financial services, and insurance (BFSI), manufacturing, healthcare, and retail being key focus verticals. In Asia, TCS has a particularly strong customer footprint in the banking, insurance, and energy sectors.

In addition, TCS is building its thought leadership by creating a broader online community, Cyber Security Community (securitycommunity.tcs.com). The community is inviting security subject matter experts (SMEs) to share their views and opinions on latest cybersecurity incidents, global trends, best practices, and snippets targeting CIOs, chief information security officers (CISOs), security professionals, and executives.

**Talent Management**

Talent management and skills development are key parts of TCS’ business strategy. In the last year, TCS has made significant investments in training its employees on digital skills, one of which is an advanced cybersecurity skill that spans across areas such as forensics, cloud security, and mobile security. TCS encourages its internal staff to cross-train and get certifications in relevant skill areas. The vendor provides not only in-house training, but also training through partnerships with major security technology vendors.

TCS also provides a Campus Commune community (campuscommune.tcs.com), an interface with academia. TCS security professionals engage with over 10,000 students, thus building a synergistic ecosystem of learning and sharing.

**Partnerships**

TCS is a part of various cloud and security associations such as SANS, Open Web Application Security Project (OWASP), Cloud Security Alliance (CSA), and ISACA. TCS partners with both upstream and downstream vendors, such as FireEye, IBM, Oracle, Forcepoint (formerly Websense), McAfee, Symantec, and so forth, leveraging their platforms and technologies to beef up its security operations for its clients and build interoperable solutions. Associations, alliances with academia, and partnerships with leading security solutions vendors constitute the focal point of TCS' strategy to provide integrated security services and always remain updated.
Customer Case

This case study illustrates how TCS' IAM expertise helped a leading financial services provider ensure regulatory compliance with a robust enterprisewide IAM framework.

One of the largest financial services holding companies in the United States was facing suboptimal performance issues with its current IAM system. Compliance concerns were growing rapidly, prompting an urgent need for an enterprisewide review and upgrade of its IAM platform.

The client organization has engaged TCS, and TCS brought in architectural changes and seamlessly integrated around 50 applications onto the new platform. The company was earlier recording approximately 40 production errors per month, which was significantly reduced to 10 per month after the engagement. The simplification of the onboarding process reduced the time taken to integrate applications onto the identity management platform. An automation process employed with the role-based access control (RBAC) approach helped expedite deployment of roles and policies. The Active directory automation further helped revoke roles, meet compliance, and recertify requirements. The user provisioning process for new employees is now completed within a day from weeks taken earlier.

FUTURE OUTLOOK

Challenges and Opportunities

The 3rd Platform–enabled DX initiatives are radically changing the way organizations engage and interact with their customers, partners, suppliers, and competitors. However, the new models of consumption, business monetization, and operations are making organizations vulnerable to more sophisticated cyberattacks and threats. As organizations increasingly adopt 3rd Platform–enabled DX technologies, they are at the risk of failing to adapt their security programs. It is becoming more crucial than ever to invest in the right security solutions and services. Furthermore, organizations are becoming conscious of the fact that they need to shift their security focus from being "preventive" to being "proactive."

In addition, IDC’s Business and IT Services Survey 2016 of over 1,300 organizations in the Asia/Pacific (excluding Japan) region suggests that end users view “enhancing security posture” as the most important theme for IT services spending in relation to DX initiatives. The survey also revealed a significant gap between the security capabilities required in the context of DX initiatives and organizations’ current state of readiness. This gap indicates untapped opportunities for security services providers such as TCS to provide more business-aligned security consulting, professional, and MSS. IDC believes that TCS has a comprehensive security services portfolio. TCS' security consulting and MSS are well positioned to provide differentiated value to its clients.

ESSENTIAL GUIDANCE

Advice for TCS

Success for security services providers will require that they implement the following:

- **Invest in local partnerships.** Partner with local security services providers, particularly in the heterogeneous Asia/Pacific region, to deliver customized solutions that address specific local regulations and business needs.
- **Deep understanding of local and the latest regulatory factors.** Many organizations' security objectives are still very much influenced by the industry or country-level regulatory environment. Security services providers have to keep track of all the latest local regulations and compliance requirements and guide clients on their implications. At the same time, providers should also invest in automation and advanced analytics tools to change the manual compliance processes.

- **Provide a flexible delivery model — security analytics as a service.** The demand for skilled data scientists who also have strong security expertise is challenging to find or retain. This presents an opportunity for the vendor to offer cybersecurity analytics and/or visualization capabilities through an "as a service" or a platform-based subscription model.

---

**LEARN MORE**

**Related Research**

- *Market Analysis Perspective: Asia/Pacific Excluding Japan Business and IT Services, 2016 — Service Delivery and Management Critical to Success in the Digital Economy* (IDC #AP41630616, August 2016)


- *IDC Asia/Pacific 2016 IT Services End-User Survey Results I: How Digital Transformation Is Changing the IT Services Market in the Region* (IDC #AP41013616, February 2016)


About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Asia/Pacific Headquarters (Singapore)

80 Anson Road, #38-00
Singapore 079907
65.6226.0330
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights.

Copyright 2016 IDC. Reproduction is forbidden unless authorized. All rights reserved.