IT OUTSOURCING VENDOR PROFILE OF:

TCS – Managed Security Services

1. Background

2. Revenue Summary

3. Key Offerings
   3.1. Security Monitoring and Incident Management
   3.2. Network security
   3.3. Vulnerability Management
   3.4. End-point security
   3.5. Identity and Access Management (IAM)
   3.6. Data Security
   3.7. Advanced Threat Protection
   3.8. Governance, Risk and Compliance

4. Delivery Capability and Partnerships

5. Target Markets
   5.1. U.S. food, agriculture, financial and industrial products sector
   5.2. U.K. Automotive manufacturer
   5.3. e-Governance Project in India
   5.4. Large European Airlines Company
   5.5. Global Healthcare and Hygiene Company

6. Strategy

7. Strengths and Challenges
   7.1. Strengths
   7.2. Challenges

8. Outlook
1. **Background**

Tata Consultancy Services (TCS) is the largest of all India-centric IT services providers, with FY 2015 (the period ending March 31, 2015) revenues of $15,454m, up 15% y/y.

In 2014, to address rising global cyber security issues, TCS consolidated its security service lines and launched a separate horizontal unit called Enterprise Security and Risk Management (ESRM). This unit offers full play of security services and solutions, including global consulting services, professional services and managed security services.

2. **Revenue Summary**

TCS’ FY 2015 revenues were $15,454m, and by region:

- North America: $8,021m (51.9% of total revenues)
- Latin America: $325m (2.1%)
- U.K.: $2,581m (16.7%)
- Continental Europe: $1,793m (11.6%)
- India: $989m (6.4%)
- APAC: $1,437m (9.3%)
- Middle East/Africa: $309m (2.0%).

The ESRM unit does not currently report as a separate P&L; revenues from the unit are currently reported as part of the infrastructure services and global consulting units, whose FY 2015 revenues were approximately:

- Infrastructure services: $2,133m
- Global consulting: $510m.

NelsonHall estimates that for FY 2015, the revenues from ESRM were ~$270m; with a revenue split across various towers as follows:

- Managed security services: ~$140m.
- Security consulting, professional services and solutions: ~$130m.
3. Key Offerings

Services offered by TCS’ Enterprise Security and Risk Management unit include:
- Managed security services
- GRC services
- Enterprise vulnerability management (EVM)
- IAM professional and advisory services
- Information protection (focused on advisory services)
- Fraud management and digital forensics (services and advisory services).

Services within TCS’ managed security services offering include:
- Security information and event management (SIEM)
- Security monitoring and incident response
- Network security
- Vulnerability management
- End-point security
- Identity and access management (IAM)
- Data security.
- Advanced threat protection.

3.1 Security Monitoring and Incident Management

TCS offers 24x7x365 security information and event monitoring of its clients’ security infrastructures. It leverages a number of technology partners for its security monitoring, log management and incident management and remediation services:
- EMC RSA
- HP ArcSight
- McAfee
- Log Logic
- Splunk
- Q1 Labs.

Through its SIEM service TCS monitors >1bn security events daily.

TCS uses a number of pre-built service accelerators including transition accelerators, process knowledgebase, dashboard, framework, threat intelligence, SOPs and reporting templates to ensure a good standard of productivity and delivery.
TCS also offers integrated SOC operations with security incident response, with end to end ownership of security incident from identification to closure. Other capabilities include forensics, incident response and malware analysis.

TCS offers SIEM and SOC services in either a dedicated managed security services model that can be tailored to the client’s context, or in a shared services model; the majority of TCS’ SIEM clients opt for a dedicated managed model.

TCS’ unified threat detection portal can be integrated with clients’ service management (ITSM) tools. TCS uses internal and external threat feeds to ensure accurate threat detection with minimized false positives. It has partnered with numerous external threat intelligence providers to provide client-specific threat intelligence, phishing detection and brand reputation monitoring.

3.2 Network security

As part of its network security services TCS offers:

- Network intrusion prevention
- Firewall management
- IDS/IPS management
- DDOS protection
- Secure remote access
- Secure web and email gateway
- Network access control.

TCS offers end to end firewall services including provisioning, management, policy management and auditing.

Network security partners for firewall, IDS/IPS and content filtering include:

- Cisco/Juniper/Palo Alto/Check Point
- McAfee/Symantec
- Websense/Bluecoat
- IBM
- HP
- Safenet.

3.3 Vulnerability Management

TCS offers vulnerability management services across application, network, platform and mobile devices. Services include:

- Enterprise vulnerability management
- Security assessment services
- Threat intelligence and advisory services.
In the enterprise vulnerability management program, TCS offers preventive, detective and response services to identify, analyze and remediate vulnerabilities in IT systems and processes.

To target areas of highest return on security investments, TCS has developed a risk based model for prioritizing the vulnerability management process.

TCS’ enterprise vulnerability management service aims to provide accurate detection of vulnerabilities through a combination of tool optimization and manual application-specific vulnerability assessment strategies, while reducing scan time via threat profiling.

As part of TCS’ integrated enterprise vulnerability management, TCS offers security architecture and design review, risk based threat profiling and modeling, and vulnerability assessment and remediation consultancy services.

TCS provides vulnerability assessment and penetration testing services through partner tools including:

- McAfee
- Qualys
- Nessus
- Rapid7
- nCircle
- Beyond Security
- IBM Appscan
- HP Webinspect.

TCS leverages in-house developed tools such as ASIDE, in addition to industry tools, to provide security assessment/ advisory services, application threat modeling, static and dynamic testing, source code review, and mobile application testing.

3.4 End-point security

Services within TCS’ end-point security portfolio include:

- Antivirus management
- Host intrusion prevention
- Integrity protection and monitoring
- Application white-listing
- Endpoint advanced threat detection and incident response
- Enterprise mobility protection
- Hypervisor security.
In its endpoint security portfolio, TCS uses a number of technologies, covering its portfolio; TCS’ primary endpoint security partners include:

- For antivirus: McAfee, Symantec, Microsoft, TrendMicro and Sophos
- For host intrusion prevention: McAfee, Sophos and Symantec
- For file integrity monitoring: Tripwire and NetIQ Change Guardian.

3.5 Identity and Access Management (IAM)

Within its identity and access management (IAM) offering, TCS provides:

- IAM consultancy and professional services including roadmapping, business case development, and IAM solution evaluation
- Deployment and management of IAM programs and technologies
- Access governance services
- Enterprise and web single sign-on
- Identity federation
- Privileged user/access management
- Identity lifecycle management: provisioning, role management, identity and access governance, audit and reporting.

For IAM services, TCS uses a number of technologies covering biometrics, smartcards and IM; the product partners include:

- CA
- Novell
- Oracle
- CyberArk
- IBM
- Dell Quest
- RSA Aveska
- Sailpoint
- PingIdentity
- Microsoft.

3.6 Data Security

TCS’ privacy and data protection include privacy impact analysis, enforcement services in terms of data leakage prevention (DLP), encryption, DRM, and certificate and key management services. Across these services TCS provides assessments, design, implementation and operations support services.
TCS also offers consulting and professional services on data privacy to help build risk management services.

TCS has developed tools around PKI, digital signature, data protection, and privacy, which are leveraged while providing security services, in addition to using third party partner tools including:

- RSA
- Seclore
- McAfee
- Symantec
- Websense
- Microsoft.

### 3.7 Advanced Threat Protection

TCS provides advanced SIEM capabilities as part of managed security services, including security analytics, threat intelligence, contextual awareness, etc. This also includes targeted attack protection, advanced malware analysis, live memory analysis, and network and host forensics.

### 3.8 Governance, Risk and Compliance

TCS’ GRC security team provides services which include regulatory and compliance management, automation of the GRC processes and programs to monitor and handle deviations, IT governance, risk management, and business resilience requirements to build resilience against business KPIs.

TCS’ technology partners for GRC services include:

- Archer
- Metric Stream
- Open Pages
- Bwise.

TCS has developed multiple frameworks which include PREMISE/cyber resilience assessment framework based on the NIST/SAN 20 critical controls, to aim to move enterprises from a compliance state to a cyber resilience state. These frameworks are focused on building the levels of defense, prevention of threats, risk maturity and recovery. TCS’ cyber resilience framework consists of the following stages:

- Compliant: documented policies and procedures
- Risk aware: instrument and automated governance processes
- Risk managed: integrated governance and security operations systems.
4. Delivery Capability and Partnerships

TCS favors dedicated SOCs operation for clients’ end to end security service delivery. It currently has 26 SOCs, 25 of which are client-specific SOCs. Each of TCS’ delivery centers are ISO 27001:2005, ISO 9000, and ISO 14000 certified, carry Cisco certified security provider recognition, and undergo periodic compliance audits.

TCS’ current multi-client SOC is based in Gurgaon and serves five clients. TCS also intends to build onshore SOCs, and has started work in the U.S., with the U.K. to follow.

TCS has 3k security professionals, of which ~80% are certified (across CISSP, CISA CISM, ISO 27001/BS 7799 Lead Auditor, CEH and product security certifications). TCS has a few associates who have also undergone the Chevening Cyber Security Fellowship Program at Cranfield University, U.K. The split of work performed by the security professionals is:

- MSS: 60%
- IAM: 19%
- EVM: 9%
- GRC: 6%
- Cloud and mobile security: 4%
- Information protection: 2%.

In FY 2015, TCS’ ESRM had ~30% growth in staff within MSS, to support the revenue growth. TCS conducts skill development programs, both internally and through technology partners, to train security employees in security tools. It also has partnerships with a number of universities including UC RiverSide, Carnegie Mellon University, Cranfield University, Stanford University, and CERT.

In the enterprise vulnerability management business, TCS’ ESRM has ~550 security testers, 120 of which perform penetration testing from six global locations. TCS also has an enterprise vulnerability management CoE laboratory in Bhubaneswar.

TCS has dedicated CoEs for MSS, IAM, EVM, GRC, and fraud and forensics at TCS’ innovation labs at Hyderabad.
5. Target Markets

TCS targets MSS within wider scope IT infrastructure engagements rather than as standalone contracts.

TCS has ~300 clients in the enterprise security and risk management business, mainly Fortune 500 companies. It has completed a total of:

- Security consultancy engagements: 500
- Vulnerability management engagements: 1k
- IAM engagements: 500
- Privacy and data security engagements: 100
- Governance, risk and compliance engagements: 400
- PKI solutions implementations: 250.

In the last FY, TCS provided managed security services to 100 clients, with ~20 end to end managed security services clients added in 2014. TCS extended or renewed 95% of clients which had contacts expiring in 2013-14. The industry split is fairly aligned with the global TCS, with BFSI being the largest sector. The largest regions are North America, Europe and APAC.

5.1 U.S. food, agriculture, financial and industrial products sector

For this U.S. food, agriculture, financial and industrial products sector client, TCS has provided end to end security services across the client’s global operations since 2013. This has involved providing services across 67 countries, from dedicated SOCs in Mexico and India. TCS provides:

- SIEM services: using QRadar across 32 appliances
- Firewall management: with Check Point for 90 firewalls, conducting bi-annual reviews of the firewalls with Tufin
- IPS: with McAfee IPS with 24 sensors
- Vulnerability management: using Qualys Guard and McAfee vulnerability managers across 12.5k IPs
- Antivirus: using Symantec Endpoint Protection for 78k users
- Incident management: using GRC Archer
- Content filtering: using McAfee Web Gateway and ISA for 61 gateways and proxies
- Endpoint encryption: using McAfee EEPC
- DLP: using RSA DLP
- Two factor authentication: using RSA and email security.

By selecting TCS and moving from insourcing its security management, the client increased the effectiveness of its security software, by using a more expansive threat database and standardizing the security tools. TCS’ services delivered productivity gains of 10%.
5.2 U.K. Automotive manufacturer

For a leading automotive manufacturer based in the U.K. with global operations, TCS provides:

- SIEM services: using McAfee SIEM
- Firewall management: with Check Point and Cisco firewalls
- Privileged access management: for Unix/Linux Servers
- Vulnerability and patch management
- Antivirus: using McAfee endpoint protection
- Content filtering: using Cisco Ironport
- Endpoint encryption: using McAfee Encryption
- Authentication: using RSA SecurID.

By selecting TCS to manage the security of the project, the client received near real-time monitoring and reporting of security events, and a reduction in time to identify and close vulnerabilities, as well as improved compliance with SOX and the organizational security policy.

5.3 e-Governance Project in India

In this mission critical e-governance project in India, TCS provides end to end managed security across a number of applications including governance, administration, endpoint security, and network security across the data center and 100+ office locations. Services include:

- SIEM services: with 200m log and 1.5k tickets per month
- Firewall and IDS: across 50 appliances
- Security audits: 200 across the data centers and offices, and 700 access controls
- IAM: for 5k users and building access controls in 80 locations
- Vulnerability management: of 250 servers and 100 network devices, with weekly scans performed by TCS
- Antivirus: across 5k endpoints.
- PKI: with the highest rate of digital certificate usage in India.

By selecting TCS to manage the security of the project, the client received a high level of security assurance and the capability to manage a high volume of cybersecurity exploits. This e-governance security implementation received recognition (twice) at national level.
5.4 Large European Airlines Company

For a large European Airline Company, TCS provides security services, focusing on:

- Security monitoring: using RSA Security Analytics
- Vulnerability management: using Rapid7 Nexpose and Metasploit
- Endpoint protection (antivirus and HIPS): for more than 6k endpoints and around 600 servers
- Remote access support: using two factor authentication for more than 10k users
- Web and email content filtering
- Data loss prevention.

Through the SIEM services TCS is able to offer near real-time alert monitoring and proactively close vulnerabilities.

5.5 Global Healthcare and Hygiene Company

For this global healthcare and hygiene client, TCS provides managed security services focused on IM. Services include:

- SOC services
- Firewall management: using Palo Alto, Checkpoint, and Cisco ASA for 92 firewalls
- IDS/IPS: using Checkpoint IPS Blade
- Identity management: using CA IM
- Vulnerability management: using AppScan and Nessus
- Antivirus: using TrendMicro across 33k endpoints.

TCS delivers user provisioning with a dedicated team to reduce the amount of time and the number of access requests, through automated provision and revocation.

Through the SIEM services, TCS is able to offer near real-time alert monitoring and proactively close vulnerabilities. By automating the provisioning and revocation, TCS has been able to reduce the number of access requests.
6. Strategy

TCS’ ESRM revenue growth towards managed security services is higher than the company average, at ~30% y/y (in line with its wider IT infrastructure services business). To continue this growth TCS intends to:

- Expand offerings to growth geographies, in particular Europe and Asia Pacific
- Develop cyber hub locations and SOCs in major markets (although its security business will continue to offer end to end security from dedicated centers). TCS intends to establish an onshore U.S. shared service SOC within the next six months, then possibly build another SOC in the U.K.
- Invest in cyber security solution centers, security operations centers, vulnerability management, and fraud and forensics labs
- Develop tools and accelerators around mobile, IoT and cloud security, to enable quicker onboarding
- Develop security frameworks, in particular around threat intelligence, fraud and forensics, and advanced SOC in addition to further development of its cyber resilience framework
- Focus on building automation and reusable tools across services
- Leverage the acquisition of IT frontier in Japan for the Asia Pacific market.

When competing against other Indian-centric providers, TCS looks to leverage its investments in identity management, EVM, fraud and forensic analysis. Against onshore providers, TCS is targeting a number of public sector contracts; it has won around four such deals in the U.S. in the last year.

7. Strengths and Challenges

7.1 Strengths

- TCS is willing to establish client-dedicated SOCs to take over the end to end management of clients’ security needs. This willingness enables TCS to support a number of clients which other Indian service providers (with primarily offshore models) are unsuitable to support
- TCS offers a number of accelerators to enable quick onboarding of clients into a managed security
- TCS’ cyber resiliency framework looks to build clients’ cybersecurity risk maturity level from reactive cybersecurity to proactively managing risks, using a number of resiliency assessments to build actionable risk mitigation plans
- TCS is able to offer a large number of penetration testers
- TCS has a large and fast growing IT infrastructure services business that it will leverage to grow its MSS business.
7.2 Challenges

- While competitive in providing end to end security services, TCS is less well suited for the deployment/provision of single security services.
- TCS’ dedicated research program into security threats is comparatively smaller than other established vendors, with research focusing on providing services at lower cost, i.e. automation, simplification and reusability.
- Although addressing the lack of shared service SOCs, TCS currently lacks security operations centers suitable for providing onsite shared services.

8. Outlook

In 2015, TCS expects enterprise security and risk management revenues to grow by approximately 25%-30% y/y. In 2015/2016, expect to see:

- TCS’ Enterprise and Risk Management unit to exist as a separately reported P&L.
- The establishment of a shared SOC in the U.S. and U.K., and the development of security-related centers in Chennai, Pune and Hyderabad.
- TCS continuing to focus on building around its objective of simplification, integration and automation for reusable services.