Presenters

Eric Hemmendinger
Senior Product Manager
Managed Security Services

Eric.Hemmendinger@tatacommunications.com
Agenda

Tata Heritage
Tata Communications Portfolio Expansion
Strategic fit for Security Services within Portfolio
Tier 1 MSSP Scorecard
Global Markets Focus – Security Services
Security Portfolio Overview
Tier 1 MSSP Scorecard Review
Q&A
The Tata Group | At a Glance

- 125 year old, Largest Private Sector Group in India
- Group includes 98 companies in 7 sectors
- Revenues FY2007 US $ 28.8 billion (3.2% of India’s GDP)
- Employees 289,500

**Group businesses are in the following 7 sectors**
- Information Systems and Communications
  - Ex. Tata Communications Limited, and Tata Consultancy Services
- Engineering
- Materials
- Services
- Energy
- Consumer Products
- Chemicals
The Formation of TATA Communications

2002
- Tata Group buys a majority stake in VSNL
- VSNL International formed – HQ in Singapore

2004
- Tata Indicom Cable (TIC) built – India to Singapore

2005
- TGN Network Acquisition

2006
- Teleglobe Acquisition

2008
- Tata Communications
# Product Portfolio

## Managed Network Services
- Private Line Services
- Ethernet WAN Services
- Global VPN Services
- Internet Access Services
- CDN
- Satellite Services
- Inbound & Outbound Voice
- ATM

## Managed Infrastructure Services
- Co-location Services
- Managed Hosting Services
- Managed Storage Services

## Managed Application Services
- Business Messaging & Collaboration Services
- Audio & Web Conferencing
- Telepresence
- Hosted Contact Centers

## Managed Security Services
- CPE – based services
  - Managed Firewall & UTM
  - IDPS
- Cloud – based services
  - DDoS D&M
  - Virtual – UTM
- ReadyMail Secure
- Token Authentication
- Vulnerability Mgmt Service
- Professional Services
- Penetration Testing
Evaluating MSS Providers

How to choose?

Weak capability 🟠 Strong capability

<table>
<thead>
<tr>
<th>Portfolio</th>
<th>Operations &amp; Delivery</th>
<th>Financial</th>
<th>Customer Service</th>
<th>Market Focus</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟠</td>
<td>🟠</td>
<td>🟠</td>
<td>🟠</td>
<td>🟠</td>
</tr>
</tbody>
</table>

Portfolio
- Breadth of Service Offering
- Depth of Technologies Supported
- Service flexibility (adaptability)
- **Measure → Customer wins**

Operations & Delivery
- Experience & Expertise of personnel
- SPOC & Local Language Support; Geographical SOC diversity
- Centralized platform, systems, tools & process
- High Efficacy security alerting
- Global CPE procurement & onsite support
- Standards based & certified (best practice)
- Reporting & service visibility (portal views for both Partner and Partner’s end customer)
- **Measure → SLA conformity**

Financial
- Price, Startup $$ and commit levels
- Enterprise Stability
- Investment level in portfolio enhancements
- **Measure → Profitability**

Customer Service
- Performance backed SLAs for both end customer experience & partner responsiveness
- **Measure → Quality rating – Customer Sat**

Market Focus
- Value prop to both SMB and Large Ent.
- Global focus with regional presence
- **Measure → Customer wins across segments**
Global Markets Focus [Security Services]

- Continued Focus on Global Enterprise markets
- Balancing roadmap strategy between developed and maturing markets
- Leverage Direct and Indirect Channels to market
- Solutions Focus
  - Protecting IP enabling services and solutions (Connectivity, VPN, MPLS, Convergence, Collaboration, Hosting & Storage)

<table>
<thead>
<tr>
<th></th>
<th>Global</th>
<th>Americas</th>
<th>EMEA</th>
<th>APAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>(Multinationals, Large National Companies)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mid Market</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>SMB</td>
<td>**</td>
<td>**</td>
<td>**</td>
<td>✔</td>
</tr>
</tbody>
</table>

** Planned via wholesale/white label with tier-2/3 providers
Benefits of Tata Communications’ Managed Security Services
Specialists in information security monitoring and management

- Supplement internal staff and skills with on-demand 3rd party expertise & best practice (ISO 27001 - ITIL - SAS-70) risk and security management systems
- Concentrate internal IT talent on projects more critical to the business; achieve better focus on strategic policy, user awareness and risk management initiatives
- Upgrade to 24x7x365 global management and monitoring with expert security analysts
- Eliminate upfront capital costs of security devices and management systems and the heavy expense of technology refresh
- Reduce ongoing operations costs of facilities, staffing & administration by +30%
- Provide your staff with the tools and process to address increasing global regulatory and complexity issues associated with managing network security
- Much like buying Insurance for your business, insure critical internet connectivity and applications from Distributed Denial of Service (DDOS) attacks
- Strengthen enterprise security posture with performance-based, money back SLA’s for realtime threat detection, policy change implementations and service availability.
- Integrate multi-vendor environments, simplify and improve reporting with enterprise-view portal dashboards and on-demand reports
Tata Communications approach to Managed Security Services
Monitored and Managed Security Solutions for your Business

**People**
- Highly experienced staff monitors your event logs 24X7X365
- Focused on monitoring & managing your security solutions
- Expertise with Blue Coat, Check Point, Cisco, Fortinet, ISS, Juniper, Tipping Point

**Process**
- SAS 70 Type I & II
- ISO 27001 Certified
- Cisco MSCP
- Single Point of Contact for customers across all Tata Communications Managed Services

**Technology**
- World class SSOC
- World’s largest DDoS D&M facility
- India’s only DDoS D&M centre
- Enabling Premise based and Cloud based security solutions
Complete range of Proactive and Defensive Security Solutions
Comprehensive Security Capabilities

<table>
<thead>
<tr>
<th>Proactive Services</th>
<th>Defensive Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed Denial of Service Defense</td>
<td>Firewalls</td>
</tr>
<tr>
<td>Token Authentication</td>
<td>Unified Threat Management</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>Intrusion Detection and Prevention</td>
</tr>
<tr>
<td>Penetration Testing</td>
<td>Email Security</td>
</tr>
<tr>
<td></td>
<td>Proxy and AntiX</td>
</tr>
</tbody>
</table>

- Insider abuse of Network Access
- Virus
- Denial of Service
- Unauthorized access to information
- Botnet compromise within organization
- Abuse of wireless network

- System Penetration
- Website Defacement
- Misuse of public web application
- Theft of proprietary information
- Exploit organizations domain name server
- Sabotage
Global Managed Security Services Portfolio
Monitored and Managed Security Solutions for your Business

**CPE-based Solutions**
- Firewalls
- Unified Threat Management
- Intrusion Detection and Prevention
- Proxy and AntiX

**Cloud-based Solutions**
- Distributed Denial of Service (DDoS) Detection & Mitigation
- Virtual UTM
- ReadyMail Secure
- Token Authentication
- Vulnerability Management

**Professional Services**
- Penetration Testing
- Consulting Services

**Supported Platforms**
- Cisco
- McAfee
- RSA
- SecurID
- IBM
- Check Point
- Juniper Networks
- F5 Networks
- FORTINET
- Google
- ARBOR Networks
- Qualys
- Blue Coat
Security Services Delivery & Operation Center

<table>
<thead>
<tr>
<th>Security Services Operation Center (SSOC)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Staffed with experienced and trained experts 24x7x365</strong></td>
</tr>
<tr>
<td>▪ Industry Certifications: ISC², ISACA, ITIL, CISSP, ISO/IEC</td>
</tr>
<tr>
<td>▪ Vendor Certifications: Cisco, Fortinet, IBM ISS, Juniper, Microsoft, Novell, Sun, Trend Micro</td>
</tr>
<tr>
<td><strong>Standards based facilities and operations</strong></td>
</tr>
<tr>
<td>▪ Built for compliance with SAS70, ISO/IEC 9000, 20000, 27001, and ITIL</td>
</tr>
<tr>
<td>▪ ISO/IEC 27001 completed</td>
</tr>
<tr>
<td>▪ Cisco MSCP certification completed</td>
</tr>
<tr>
<td>▪ SAS 70 – Type 1 &amp; 2 complete</td>
</tr>
<tr>
<td><strong>Single Point of Contact for all services</strong></td>
</tr>
<tr>
<td><strong>Multiple Contact Options available 24x7x365</strong></td>
</tr>
<tr>
<td>▪ Telephone</td>
</tr>
<tr>
<td>▪ Electronic (Web, Email, IM/Chat, etc..)</td>
</tr>
<tr>
<td><strong>State-of-the art security intelligence and event management capabilities</strong></td>
</tr>
<tr>
<td>▪ Leveraging a technology integration/partnership with IBM ISS</td>
</tr>
</tbody>
</table>
CPE-based Security Services

- **Firewalls**
  - Flexible service models
  - Leading vendors / technologies
  - Full service on-demand portal

- **Unified Threat Management**
  - Integrated security device
  - Flexible service model
  - Leading vendors / technologies
  - Full service on-demand portal

- **Intrusion Detection and Prevention Systems**
  - Flexible service models
  - Leading vendors / technologies
  - Full service on-demand portal

- **Global Services, Local Expertise**
- **End-to-End Visibility Management**
- **Speed, Customization, Scalability**
### Cloud-based Security Services

#### Global Services, Local Expertise

**Virtual UTM**
- Full featured UTM in the cloud
- No Security CPE
- We own & manage the security device
- Subscription based model, easy to subscribe and implement

**DDoS Detection**
- Network deployed across global IP backbone
- Deep packet inspection with real time IP traffic analysis and notification
- Dedicated IP circuit speeds supported up to 10 GB

#### End-to-End Visibility Management

**Token Authentication**
- Available worldwide
- RSA and mobile device options
- Centralized management
- Replaces weak password security

**DDoS Mitigation**
- Network deployed scrubbing centers directly on global IP backbone
- Multi-gigabit scrubbing capacity
- Carrier class architecture
- Fully integrated with DDoS Detection service

#### World’s largest DDOS D&M infrastructure

**Vulnerability Management Service**
- Comprehensive identification, classification & prioritization for vulnerabilities
- Network devices and servers
- Tata-managed or customer self-managed

**Ready Mail Secure**
- Help eliminate threats before they reach your network
- Activate quickly with a simple MX record change
- Deploy quickly without up-front capital investment
Professional Security Services

Consulting Services
- Delivery through a regional network of technology partners, including Tata Consulting Services (TCS)

Penetration Testing
- Includes Wireless, Network and Application assessments
- Full service testing with complete, comprehensive and customizable reports

End-to-End Visibility Management
- Speed, Customization, Scalability

Global Services, Local Expertise
Product Overview

Virtualized Unified Threat Management
ReadyMailSecure
Vulnerability Management Service
Penetration Testing
Token Authentication
Virtualized Unified Threat Management

Features

- An integrated ‘All-In-One’ cloud-based Security service (Firewall, Anti-Spam, Anti-Spyware, Anti-Virus, IPS & Web filtering)
- No Security CPE. We own and manage the security devices.
- Internet traffic is scanned and cleaned before it reaches customer premise

Benefits

- No investment in Security CPE
- Subscription-based model. Easy to subscribe and implement
- 24x7x365 management & monitoring by expert security staff
- Secure remote connectivity through IPSec-based client and site-to-site Virtual Private Networks.
- Log management & analysis using industry-leading technology from Fortinet
Features

- Helps eliminate viruses, protecting your infrastructure and data and boosting employee productivity
- Helps reduce spam dramatically preserving network bandwidth and storage by reducing email volume
- Helps filter out inappropriate content, protecting users and your company image by detecting unacceptable images
- Disaster recovery – 7 days unlimited queue management

Benefits

- Helps eliminate threats before they reach your network
- Never lose inbound mails
- Deploy quickly without upfront capital investment
- Integrate with your existing e-mail setup
- Govern use of the e-mail system and help prevent misuse
- On demand scalability

Email Without the Email Security Service

Email Flow With the MailSecure Service
Features

- On-demand service that provides discovery, policy creation, scanning, reporting, and remediation workflows to quickly and accurately identify and remediate security vulnerabilities.
- Customized scans for specific ports, services, and/or vulnerabilities match scanning activity to the relative importance of each device.
- Customized timing of scans balances network and device bandwidth consumption against system performance requirements.
- Customized reports provide comprehensive information for IT staff for rapid decision-making on remediation.

Benefits

- Turnkey deployment requires no software to install, update, or maintain, and offers lowest cost of operation.
- Proactive, early warning, security intelligence prevents unnecessary downtime.
- Structured, auditable procedures detect security vulnerabilities and reduce business risk.
Penetration Testing

**Features**

- Test against a wide range of attacks types, vulnerabilities & tactics
- Identify devices, systems, applications and services that may be potential attack targets
- Simulated test with real world tools and tactics
- We use cutting edge tools and tactics (to keep up with those used in the hacker community)
- We assess vulnerabilities using a variety of exploit techniques
- Our testing can include all 7 layers of the OSI stack

**Benefits**

- Discover and address vulnerabilities before criminal activity occurs
- Understand the level of exposure and business impact of security breaches
- Reduce the impact and frequency of security incidents
- Meet compliance and regulatory requirements requiring periodic security assessments
Managed Token Authentication

Features

- Secure internal and remote access to corporate network with an easy to use portable solution
- Strong two-factor authentication is more secure than passwords
- All communication between the server and agents on the protected device are encrypted using RC5 (RSA proprietary algorithm) or DES

Benefits

- Accelerates speed to protection by providing rapid and cost-effective deployment of strong authentication and allows secure and fast on-boarding of users
- Helps minimize business impact and improve security posture by preventing unauthorized access within and outside the organization
- Helps reduce complexity of deployment, staffing requirements, administrative & logistics overhead, user management & infrastructure costs for lower total cost of ownership
- Allows organizations to provide remote access and expand business with trust in transactions
Thank You

Backup Slides
Managed and Monitored Firewall and Unified Threat Management

Features

- Customized Planning, Design & Configuration of contracted firewall & UTM devices
- Support for site-to-site or remote access VPNs using IPSec
- All-in-one capabilities with UTM, including Anti-Spam, Anti-Virus, VPN, Intrusion Prevention and Content filtering

Benefits

- Minimize risk of business-impacting security breaches
- Meet industry certification & regulatory compliance guidelines
- Increase coverage levels through 24x7x365 management & monitoring by experienced security engineers
- Use resources more efficiently with an all-in-one UTM solution
Managed Intrusion Detection and Prevention System

Features

- Multi-vendor platform support (3com, Cisco, McAfee, IBM..)
- Full life cycle monitoring, management & maintenance
- Security Incident escalation
- Near real time reporting includes event logs, threat analysis, news and alerts

Benefits

- Improve awareness and minimize the extent of business-impacting security breaches
- Reduce security administration overhead and achieve more efficient use of internal staff
- Increase coverage levels through 24x7x365 management and monitoring by experienced security engineers
Distributed Denial of Service (DDoS) Detection and Mitigation

Features

- World’s largest deployment of DDoS detection & mitigation capabilities (Arbor Networks)
- A network-based service scrutinizes your network traffic in real time to identify anomalies and quarantine attack packets
- Only malicious traffic is blocked – legitimate traffic continues to flow through so your network and applications remain available to legitimate users

Benefits

- Bypass traditional, tedious fault resolution procedures with monitoring and notifications
- Enjoy lower total cost of ownership as against premise-based solutions
- Be prepared for a range of attacks with mitigation based on maximum attack size, not bandwidth
- Protect last mile bandwidth & avoid costly over-provisioning
# SSOCC Personnel Credentials

<table>
<thead>
<tr>
<th>Certifications</th>
<th>Certifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certified Information Systems Security Professional (CISSP)</td>
<td>Checkpoint Certified Security Administrator (CCSA)</td>
</tr>
<tr>
<td>Certified Information Systems Auditor (CISA)</td>
<td>Checkpoint Certified security Expert (CCSE)</td>
</tr>
<tr>
<td>Certified Novell Engineer 4.11 (CNE)</td>
<td>Certified Tipping Point Intrusion Prevention System</td>
</tr>
<tr>
<td>Cisco Certified Network Associate (CCNA)</td>
<td>Certified and trained on Nortel Passport 8600 Configuration and Management</td>
</tr>
<tr>
<td>Cisco Information Security Specialist</td>
<td>Fortinet Certified Network Security Associates (FNCSA)</td>
</tr>
<tr>
<td>Cisco Firewall Specialist</td>
<td>Juniper Networks Certified Internet Associates (JNCIA-FWV)</td>
</tr>
<tr>
<td>Cisco IPS Specialist</td>
<td>Juniper Networks Certified Internet Specialist (JNCIS)</td>
</tr>
<tr>
<td>Cisco Certified Design Associate (CCDA)</td>
<td>ITIL V3 Foundation Certification</td>
</tr>
<tr>
<td>Cisco Certified Network Professional (CCNP)</td>
<td>ISS Certified Product Specialist in Real Secure</td>
</tr>
<tr>
<td>Microsoft Certified System Engineer (MCSE)</td>
<td>ISS System Scanner and Internet Scanner</td>
</tr>
<tr>
<td>Microsoft Certified Professional (MCP)</td>
<td>Trend Micro Level 1 Internet Validated Technician</td>
</tr>
<tr>
<td>ISO27001 Implementer</td>
<td>Sun Certified System Administrator Part I &amp; II – 2.7</td>
</tr>
<tr>
<td>BS7799/ISO 27001 Internal Auditor</td>
<td></td>
</tr>
</tbody>
</table>
A leading equities and securities firm in India is a prime example of a bank that had to innovate to enhance security. The firm’s IT department was growing increasingly concerned about repeated distributed denial of service (DDoS) attacks against its network.

Although an existing firewall solution was installed, the equities and securities firm was determined not to fall prey to a massive DDoS attack that could cripple its network and halt online banking activity for hours or days. The firm’s IT department realized that building a DDoS mitigation solution would take time, expertise and resources that were not available in-house.

Why Financial Services firm's choose Tata Communications

- First global service provider from India to achieve Cisco® powered status for Managed Security Services
- Tata Communications has deployed the world’s largest DDoS mitigation infrastructure
- Full range of monitored and managed security solutions that are backed by aggressive, performance-based Service Level Agreements (SLAs)
- Real-time security monitoring and management options at a fraction of the cost of in-house or competitive solutions
- High-quality, cost-effective security services, which include premise and cloud-based offerings as well as professional services, enable Tata Communications to provide customers with security solutions on a global basis.
Case Study – Golden Boar

End-to-end network solution with built-in security

Background and Industry
Golden Boar Alderney Limited, an online casino, is located in the British Channels Islands yet hosts practice sites in Asia. The company was growing increasingly concerned about reports of Distributed Denial of Service (DDoS) attacks against online gaming companies in China, Taiwan, and the Philippines.

Business Challenges
Hackers launch DDoS attacks to prevent legitimate use of service, such as flooding a network with spam email or disrupting connections between machines to deny users access. These attacks are also used to extort money from businesses by threatening an attack if payment is not made.

Network engineers at Golden Boar were determined to prevent DDoS attacks so when it came time to add an additional practice site in Singapore, the company chose Tata Communications’ Dedicated Internet Access (DIA), that offered sophisticated bundled security options.

The Solution
Tata Communications’ round-the-clock network and security operations centers now monitor Golden Boar’s network infrastructure. In this way, Golden Boar stays focused on running its casino operations while Tata Communications delivers protected service.

To ensure that Golden Boar is fully aware of threat levels and risks, Tata Communications provides access to a security portal for real-time reporting and advanced security assessments.
Online Security Assessment Tool

Visit www.tatacommunications.com/security/assessment

- Conduct a Self Assessment
- Obtain an Immediate and Custom Report
- Identify areas of focus
- Identify best practices and recommendations
- Collaborate with Tata Communications to secure your business!
Service Level Agreements (SLA’s)

*Industry leading, performance-based SLAs Proactively reported, with financial remedies applied*

- **Security Incident Performance Guarantees**
  - Incident Identification
  - Incident Response
  - Internet Emergency
- **Policy Change Performance Guarantees**
  - Change Acknowledgement
  - Change Implementation
- **Lifecycle Management Guarantees**
  - Service Implementation
  - Proactive System Monitoring
  - Proactive Security Content Update
Thank You

Questions?

For Further Information Contact:

Janice Goveas
janice.goveas@tatacommunications.com