IDC ANALYZE THE FUTURE

IDC TECHNOLOGY SPOTLIGHT

This IDC Technology Spotlight attempts at drawing a realistic scenario of the challenges faced by Indian CIOs and CISOs in the country today in cybersecurity, and how managed security services can increasingly contribute to allaying these issues. The document also highlights how Indian organizations can engage with Tata Communications to accomplish high levels of security and compliance, thus leading to business continuity and near-zero business disruption and losses.

Securing the Digital Transformation Journey — The Pivotal Role of Managed Security Services

December 2018
Sponsored by: Tata Communications

Written by: Ranganath Sadasiva, Research Director; Sandeep Kumar Sharma, Associate Research Manager

I. Introduction

As digital transformation (DX) continues to garner a lion's share of organizations' IT budgets, a pertinent issue that has been brought to the forefront in the last 12 months is how can organizations ensure the security, compliance, and resiliency of the overall DX infrastructure.

Indian organizations are estimated to spend nearly 25% of their 2018 ICT budgets on digital transformation initiatives, as per an IDC study, Decoding DX, published in January 2018. Companies across several industry verticals and sizes have jumped on the DX bandwagon to accomplish benefits accruing from such initiatives and to stay relevant vis-à-vis their competitive ecosystems.

The Indian market is interspersed, with most of the larger organizations leveraging a hybrid cloud infrastructure. Public cloud services have been a key enabler for DX programs and accounted for a spend of US$1.5 billion in CY17 (as per IDC's Public Cloud Services Tracker, 2H17). This amounts to roughly 58% of organizations in India having adopted software as a service (SaaS) and 41% of organizations having implemented infrastructure as a service (IaaS) in 2017 (Source: IDC India CloudView Survey, 2017).

Larger Indian organizations have also moved toward deploying a private cloud setup, especially for their mission-critical applications — an estimate pegs the enterprise private cloud (for large and very large organizations) adoption by 59% of

AT A GLANCE

KEY THEME

DX is driving cybersecurity spending; however, there needs to be a consolidated and coordinated approach toward security, risk, and compliance.

WHAT'S IMPORTANT

Companies are plagued with an acute shortage of cybersecurity professionals and a daunting task of managing a complex and ever-growing security infrastructure. The rapidly evolving threat landscape completes the triad of cybersecurity challenges.

There needs to be a thrust on leveraging the services of managed security services providers (MSSPs) to secure digital assets 24/7, and for effective detection and response.

companies. IDC expects the growth trends in the cloud market to continue, with IaaS slated to grow at a compound annual growth rate (CAGR) of 34% for the 2017–2022 period (this is almost 2.5x of the overall software market growth for the same period).

In a similar vein, Indian organizations have been quick enough to adopt emerging technologies, such as Internet of Things (IoT) and cognitive. An IDC IoT Spending Guide 2H17 pegs the CAGR in the overall IoT market in the country to be 10.6% for the 2017–2022 period, with IoT software and allied services slated to grow higher than the market for the same time frame.

Improvement of business productivity and reduction of operational costs were the top drivers for IoT implementations in India in 2017.

The rise in maturity of business processes has also led organizations to implement analytics and cognitive solutions. The spend on analytics solutions stood at US$1.3 billion in 2017 and is slated to grow at a CAGR of 15.8% for the 2017–2022 period (Source: India IT Spending Guide, 2H17). The interest among Indian organizations toward cognitive solutions is also very high, with a significant majority of larger organizations having already deployed cognitive on a pilot scale. Front-runners for adoption of such solutions are organizations in technology, telecommunications, media, and BFSI industry verticals.

II. How Do Indian Companies View Security as a Part of Their DX Journeys?

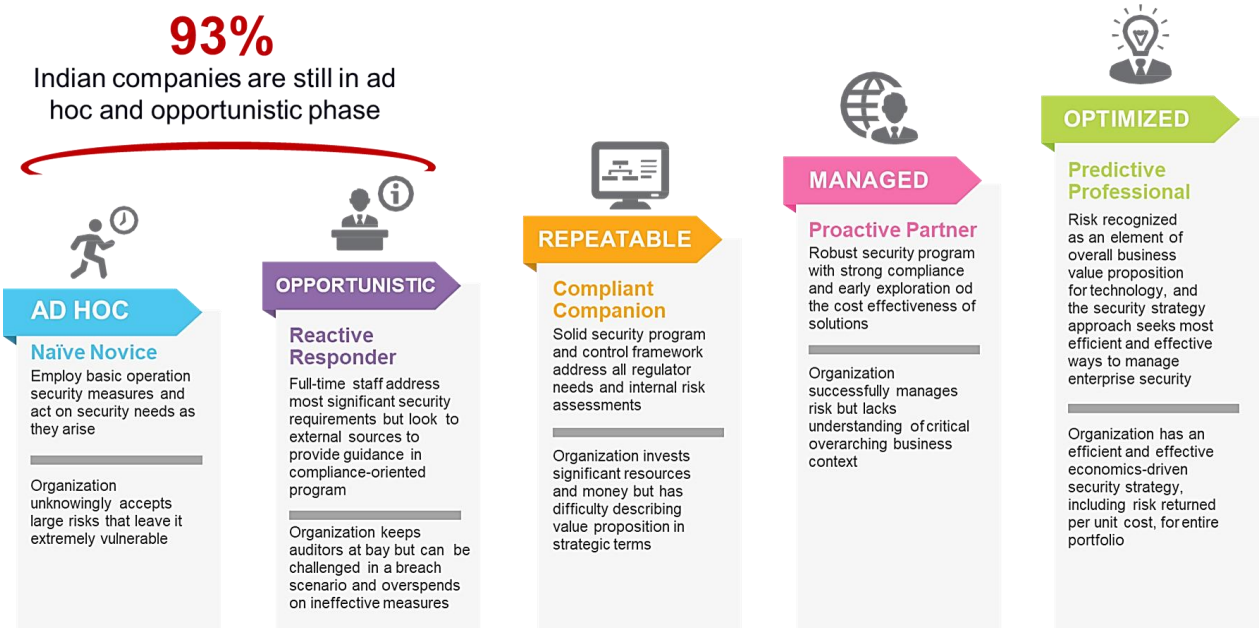
The year 2017 was phenomenal in adding to the awareness of the importance of cybersecurity among Indian companies. In the last 12–18 months, companies have experienced several data and security-related breaches, with the most notable one being led by the ransomware attack last year. This has led Indian organizations to consider cybersecurity with a heightened level of importance and to appreciate the urgency of actions in this regard.

49.3% of the companies spent the largest on security as a part of their DX implementations in 2017. (Source: IDC DX Executive Sentiment Survey, 2018)

Despite the rise in awareness and consequent security-related spending, Indian companies are relatively immature in forging a coordinated cybersecurity strategy to protect their digital assets. An IDC Security MaturityScape (2017) estimated that 93% of Indian organizations are still in the initial phases of cybersecurity maturity. In such organizations, adoption and spending is still on point security solutions, with a lack of a central cybersecurity strategy; dearth of a compliance framework with

KPIs is the order of the day; organizations face an acute shortage of cybersecurity professionals to implement and manage the security infrastructure; leadership sponsorship toward security is lackadaisical.

FIGURE 1: *IDC India Security MaturityScape — Assessing the Cybersecurity Maturity of Indian Organizations*



Source: IDC India Security MaturityScape, 2017

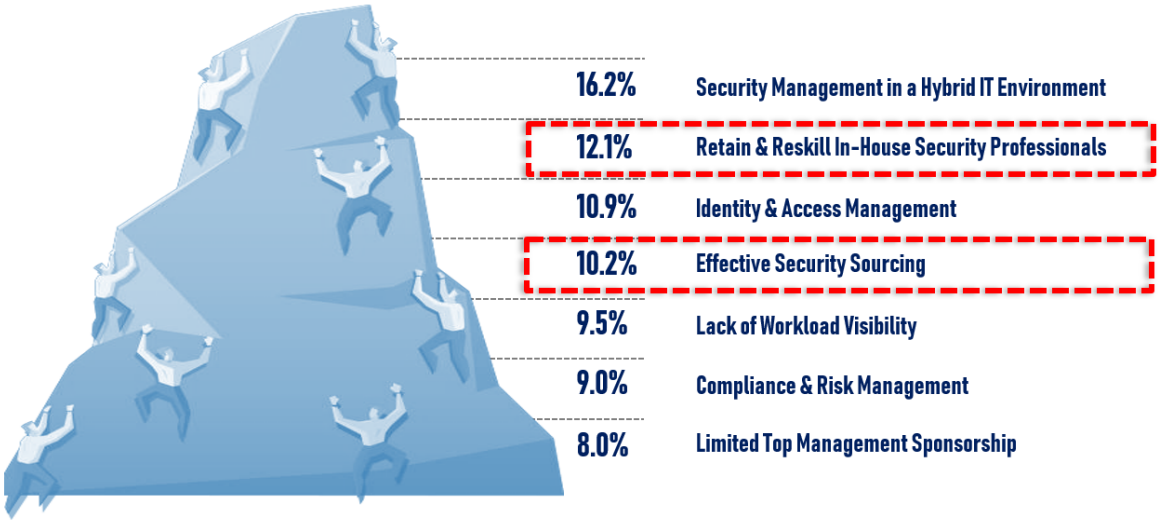
III. Security-Related Challenges Faced by Indian Organizations

Indian companies face several challenges w.r.t. their security infrastructure, the most notable of these being an acute shortage of cybersecurity skilled professionals (including the challenge to reskill and retain the existing ones in the organization). This can lead to mismanagement of applications and infrastructure, opening avenues of vulnerabilities and increasing the threat surface, ultimately leading to breaches. 24/7 monitoring and incident response are critical to protecting organizations' assets and in the absence of such resources, organizations are bound to place their business reputation and, ultimately, value at risk.

Coupled with this, organizations are also grappling with effective security sourcing strategies and have to contend with handling more than 25 security vendors (on an average). This leads to

lowering of productivity levels of the in-house IT and security team and adds to the complexities of managing such humongous security infrastructure.

FIGURE 2: *Major Security-Related Challenges Faced by Indian Organizations*



Source: IDC IT Services Survey, April 2018, N= 98

IV. Companies Need an Integrated Cybersecurity Approach — The Future Lies in Managed Security Services

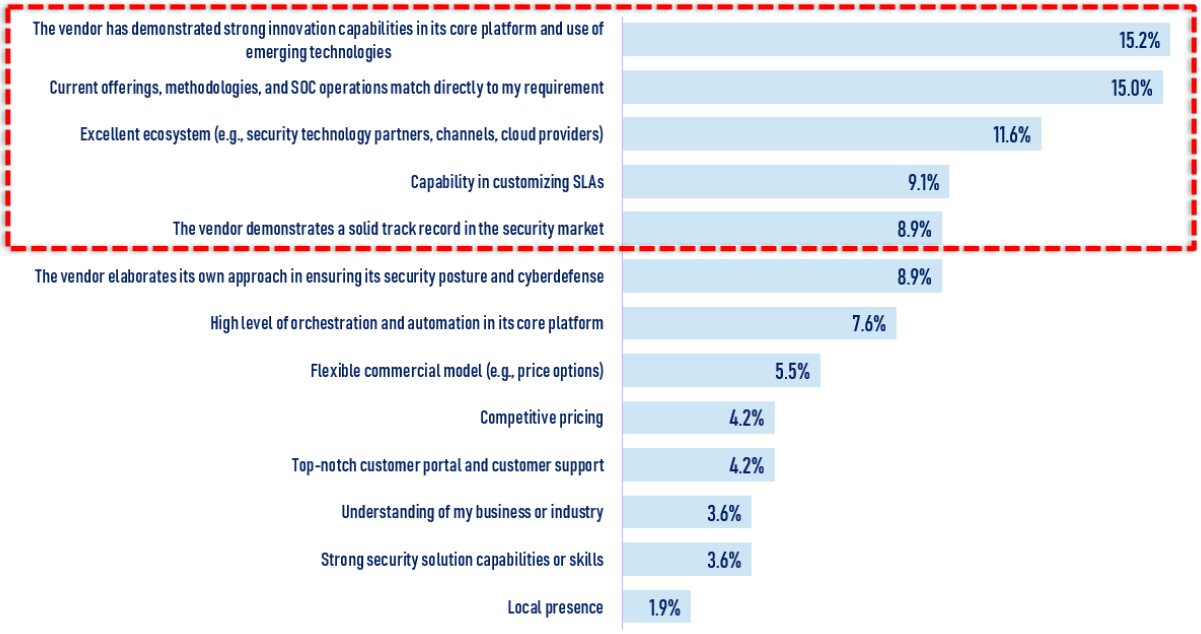
As more and more organizations continue to face increasingly sophisticated cybersecurity attacks, intensified by digital technologies, especially mobile and IoT, IT security teams require a new IT strategy that encompasses powerful new tools to protect data and infrastructure. Companies now need a portfolio of security solutions that are fully managed by a service provider and which are geared toward meeting the IT and business goals and objectives of a client organization.

This has propelled an increasing demand for managed security services, which is being boosted not only because of the increasing instances of cyberattacks on enterprises, but also because of the stringent government regulations and the growing BYOD trend among organizations. An MSSP can stitch together various security components to forge the requisite solution with an integrated architecture; bring in the best-of-the breed solutions and methodologies; and ensure effective operationalization, management, and 24/7 monitoring, detection, and incident response through the skilled cybersecurity professionals pool.

V. Selecting the Right MSSP

The threat landscape has completely evolved; hence, organizations expect MSSPs to demonstrate strong innovation capabilities and to leverage emerging technologies, such as automation, machine learning, and analytics in the delivery of security services. Additionally, the MSSP must be able to deliver a comprehensive solution, securing diverse infrastructure components ranging from network, applications, data, IoT, and other endpoints.

FIGURE 3: *MSSP Selection Criteria*



Source: IDC IT Services Survey, April 2018, N= 98

One of the other top selection criteria is the ecosystem approach of the MSSP — this is an interconnected world in which the MSSP has to have a link with numerous partners (application and infrastructure providers, security software and appliance providers, and nice players and start-ups in the security segments).

A major part of offering managed security services is setting up of security operations centers (SOCs). A reliable partner must have established several SOCs around the world, from which skilled manpower would be able to monitor, manage, and mitigate the threats, cyberattacks, and breaches in real time 24/7/365. There is a huge skills gap in cybersecurity, coupled with a lack of

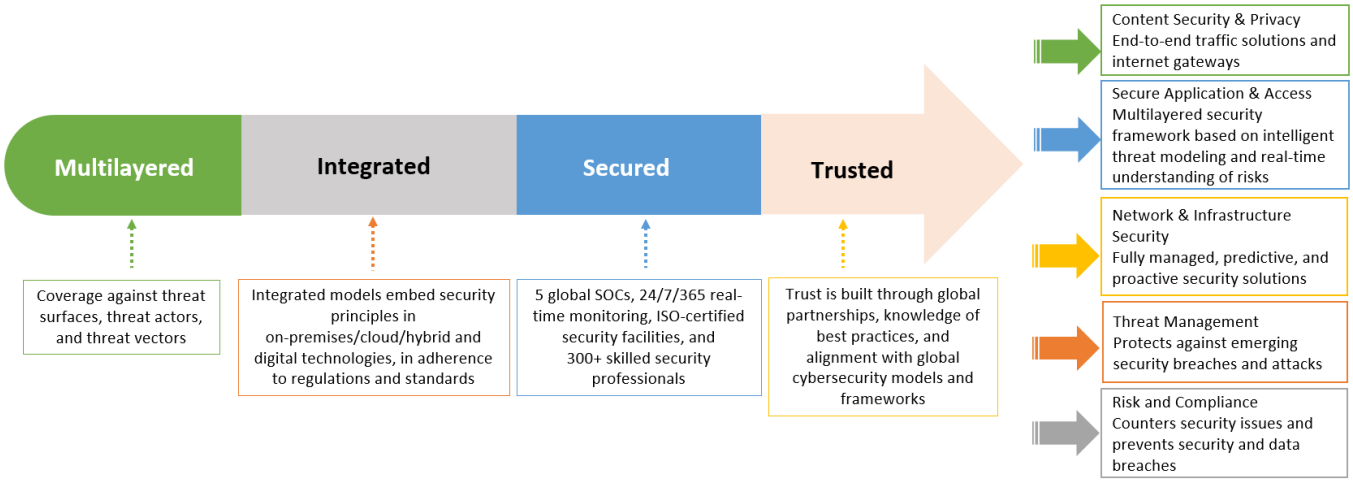
awareness among enterprises on the kinds of risks and the tools to mitigate them. A reliable partner must have the requisite knowledge, experience, and expertise of being able to formulate accurate IT security strategies that are in line with the client organization's specific needs and have the necessary security experts to put together the requisite tools to keep the business secure.

VI. Considering Managed Security Services from Tata Communications

Tata Communications is one of the leading digital infrastructure solutions and managed security service providers in India and globally. It provides an integrated managed security services portfolio that helps its users to build and monitor cybersecurity programs and provides its users with a real-time view to predict, identify, prevent, detect, and respond to cyberattacks.

Tata Communications offers solutions that cover various layers of the information and digital systems stack.

FIGURE 4: *Tata Communications Managed Security Services Portfolio*



Source: Tata Communications

Tata Communications helps organizations to protect against cyberthreat vulnerabilities by focusing on aspects of the following: **content security and privacy, secure application and access, network and infrastructure security, threat management, risk and compliance, and advanced security.**

Content Security and Privacy

Tata Communications provides traffic solutions and secure internet gateways to protect organizations' digital business against external threats, offer reliability, and ensure near-zero business disruption. It seeks to protect enterprises' content and privacy through four pay-per-use cloud-based solutions:

- Global secure internet gateway offers coverage for common security issues through basic security tools, such as firewall, antispam, antivirus, IPS, VPN, and web filtering.
- Global secure web gateway provides complete visibility of all the web-based activity across the enterprise, including branch offices, datacenters, internet gateways, home workers, and mobile workers. It deploys security policies uniformly for users across the organization and scans and cleans the incoming internet traffic to protect against threats.
- Global secure messaging gateway protects data and users from spam, viruses, and malware before any damage and can be deployed quickly with no up-front capital investment.
- The data leak prevention service allows users to monitor and manage the flow of data to prevent leaks to unauthorized people through cost-effective compliance reports.

Secure Application and Access

Tata Communications offers a multilayered security framework that is based on intelligent threat modeling and real-time understanding of risks, including user authentication. The six solutions under this segment protect organizations from application layer and network attacks:

- The Advanced Malware Detection solution is a fully managed, flexible, and multilayered approach that allows users to choose the required level of protection they need to counter cyberthreats. It also allows users to choose between endpoint, network-based, or hybrid to detect and block advanced malware.
- The Web Application Firewall solution analyzes Layer 7 application traffic, monitors target applications, and inspects all inbound and outbound traffic. The Web Application Firewall based on the security information and event management (SIEM) platform offers visibility, detection, and protection against web application and OWASP Top 10 vulnerabilities.
- The Guest Wi-Fi Access cloud-based solution is an end-to-end solution for secure, always-on connectivity. It manages web access policies, users, time, quotas, and bandwidth. The outbound firewall, antivirus, and antimalware includes advanced security capabilities, such as authentication and transaction log storage for a minimum of six months, and multiple authentication techniques.
- The Remote User Authentication solution offers a two-factor authentication platform for globally distributed teams. Among the main features of the fully managed platform are a user-created personal identification number and a randomly generated code to ensure account safety. Other features include a 24/7 service desk support and cloud-based scalable modes, based on fully managed authentication servers.

- The Cloud Access Security Broker uses advanced technologies, such as machine learning algorithms, for various capabilities, such as user anomaly detection, data leakage prevention, configuration monitoring, tokenization, encryption, cloud risk governance, and device profiling. It enforces security policies across SaaS, PaaS, and IaaS cloud services, which offer protection against threats, ensures compliance, offers data security, and provides visibility.
- Identity as a Service is another solution under this segment, which provides secure access in both hybrid cloud and onsite delivery models. It is an interface for employees, customers, and partners, enabling them to connect to all the applications securely, thus offering interoperability and integration across private and public cloud, as well as mobile and IoT.

Network and Infrastructure Security

Tata Communications is offering four end-to-end fully managed security services that deliver real-time detection and mitigation of risks:

- The Firewall and Unified Threat Management service offers monitoring and management of firewalls from Tata Communications' SOC for 24/7/365 availability.
- The Distributed Denial of Service (DDoS) Mitigation solution offers defense against complex high volume and application layer DDoS attacks, thus protecting critical assets, such as the datacenter and business-critical applications, and offering real-time detection and mitigation.
- The Intrusion Detection and Prevention Service is an early warning system that proactively detects threats and attacks on a 24/7/365 basis.
- The Firewall Audit and Optimization service simplifies network security management with a fully managed optimization.

Threat Management

Tata Communications' Threat Management portfolio is a leading global solution with advanced detection and mitigation capabilities for emerging security breaches and attacks. The SIEM platform is for managing business risks through alert mechanisms and customized information security policies. The Cloud SIEM platform is for detection of security issues in real time and for responding to the incidents as quickly as possible.

An integrated, centralized dashboard provides visibility into attacks against the client organization's infrastructure and churns out intelligence insights for mitigation against these threats, thus enabling compliance. The SOC Portal offers a single view dashboard with snapshots and threat trends over time. Its real-time analytical reporting offers actionable insights and better viewpoints for CIOs and CTOs to make meaningful security decisions. The Advanced Threat Protection solution uses analytics and machine learning to detect patterns and anomalies to discover newer kinds of threats and provide monitoring with advanced correlation rules.

Risk and Compliance

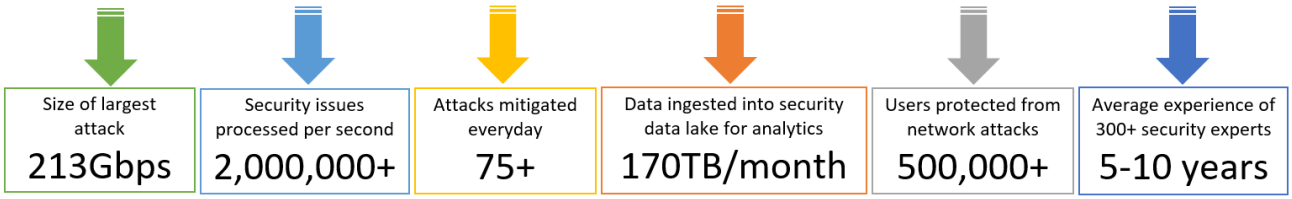
Tata Communications offers risk and threat management services that prevent potential security and data breaches, thus helping organizations to reduce the impact of security incidents and minimize business losses.

- The Vulnerability Assessment and Penetration Testing solution offers a 24/7 on-demand scan of the organization's network and web applications to detect threats and risks. It detects security vulnerabilities and reduces business risk by pre-empting existing vulnerable exploits and preventing business downtime.
- Tata Communications also offers Governance, Risk, and Compliance Consulting, covering security risk and assessment consulting, compliance assessment and planning, and data privacy assessment. It offers an assessment of the client organization's current security setup and identifies gaps, and then ensures that the organization's data processes meet the requisite regulatory compliance requirements.

VII. Differentiating Factors — Why Tata Communications?

Tata Communications is an industry leader in the managed security services segment in India and globally. With its multiple levels of support across different technologies and companies, and industry certifications (such as CISSP, CISM, SANS, CISA, CCNA, CCNP, MCSE, SNIA, F5 LB, PMP, ISO/IEC, ISAE, ITIL), it presents a strong case in the highly competitive market. Tata Communications has some numbers to report, represented in Figure 5.

FIGURE 5: *Competitive Differentiation of Tata Communications as an MSSP*



Source: Tata Communications

- Apart from its industry-leading experience and expertise gathered over the years, Tata Communications operates a Cyber Security Response Center (CSRC) in Chennai, which offers comprehensive SOC capabilities, technologies, and processes. The center showcases live demos of processes, maintenance, and dashboards.

- Including the Chennai CSRC, Tata Communications has set up four global CSRCs or SOCs in the region with data residency to provide localized managed security services and has a dedicated MSS test lab set up for technology evaluation and simulation.
- Further, Tata Communications has partnered with 24 DDoS scrubbing farms globally, as well as with several leading global technology providers. Tata Communications has a customer portal and reporting application, interfaced with in-house ITSM.
- Tata Communications has a clear-cut approach toward handling security through a well-articulated and integrated framework, on which a range of solutions and platforms are built upon.
- With a platform-based model, it goes beyond deploying vendor/OEM-specific products and follows the best-fit approach and aligns with global security and privacy solutions and frameworks.

VIII. Demonstrated Implementations

Tata Communications boasts of a strong clientele across India and internationally that is leveraging its managed security services portfolio and have managed to garner significant benefits. Table 1 highlights some key customers, their security needs, Tata Communications solution, and impact accomplished from the services offered.

TABLE 1: *Cases in Point*

Customer Industry Vertical	Business Objective (Problem)	Expected IT Outcomes	Action Taken (Tata Communications Solution)	Results Achieved
Manufacturing	Security issues for web applications and layers, difficulty in managing security infrastructure in-house, inability to meet growing user base requirements, manageability issues in using multivendor solutions	Multivendor solution management, log management, and reporting dashboards	• SIEM solution combined with an SOC setup • Cloud DDoS solution • Secure Web Gateway solution	24/7/365 centralized monitoring and management for existing security infrastructure

Banking	Build a next-generation in-house SOC with 25+ advanced security controls, and an on-premises monitoring and management system	Leverage existing security setup, to reduce future efforts for upgrading and integration of platforms, mitigate cyberattacks, and align skilled resources for end-to-end management of SOC infrastructure	Design, build, and manage an on-premise SOC, incorporating multilayered solutions	Multilayered security products and services coverage provided by deploying SIEM, GRC, APT protection, and decoy services; Enterprise Security Architecture and process definitions laid down
Retail payments and settlement systems	Counter cyberthreats and zero-day attacks, track and mitigate security issues, monitor logs from three datacenters, provide forensic analysis, systems integration, support for Incident Management workflow and CA service desk	Devices integrated across three different locations, devices and logs integration, and detect real-time deviations	• Micro Focus ArcSight as the on-premises SIEM solution • Blue Coat Security • Onsite security SME	Better identification and mitigation of attacks; effective implementation of the SIEM solution through dashboards, reporting and notifications, and PCI and ISO 27001 compliance modules
IT and ITeS	Network faced multifocused DDoS attacks at speeds of up to 200Gbps, choked bandwidth, and network downtime of 6 days	Handle harmful traffic and scrub the malicious packets to deliver legitimate traffic, thereby supporting restoration of critical services, freed up bandwidth	DDoS protection service	Optimal network performance, protection against cyberattacks, threat monitoring, and real-time threat escalation
IT and ITeS	Decentralized legacy technology infrastructure, high risk for cyberattacks, low network availability, challenge to make business-critical applications safely available, and SLA manageability issues	Centralize all disparate network systems and link all RBEI offices across India onto a single platform, requisite capacity and scalability	vProxy unified threat management solution, based on a secure proxy solution that leverages cloud	Centralized secure network, comprehensive IT and network cyber protection

Source: IDC, Tata Communications

IX. Concluding Remarks — Recommendations to the CISO Community

The Indian market is currently witnessing a paradigm shift w.r.t. transformation projects, and this calls out for similar exercises in securing these projects. Business leadership and the CISO community must appreciate the significance of cybersecurity, compliance, and risk management toward the health and business value of their organizations.

- Leadership vision and sponsorship for raising the cybersecurity posture is the first and one of the most critical steps in the DX journey. CISOs must carefully examine their current positions (w.r.t. security) through assessments conducted internally and validated through industry bodies and MSSPs. Without this assessment, it would be impossible for them to understand and place emphasis on the future goals, strategies, and tactics in place.
- Consolidation should be the mantra for organizations — security infrastructure must consist of the best-of-the-breed comprehensive solutions and, at the same time, must be consolidated and simplified enough for adequate management.
- Perpetual vigilance must be adopted for security measures and processes — 24/7 monitoring, detection, and response tools/services must be leveraged by organizations without fail, considering the fact that it is business reputation that is at stake.
- Dealing with the current threat dispensation, organizations must leverage emerging technologies, such as cloud, artificial intelligence, automation, and analytics in their security infrastructure.
- With regard to cybersecurity professionals, companies must either build or leverage skills (of external parties). The former can take a much longer time frame; hence, organizations must immediately beef up their cybersecurity professionals resource pool for effective monitoring, detection, and remediation.

IDC TECHNOLOGY SPOTLIGHT

About the analyst: Ranganath Sadasiva
Director - Research, IDC India

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

5 Speen Street
Framingham, MA
01701, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com