This paper will share insights on factors driving adoption of managed security services among Indian organizations as well as benefits and risks associated with it.

Rishikesh Kamat, Netmagic Solutions

Organizations across a wide variety of industries are turning to cloud computing to manage their infrastructure growth, reduce costs, decrease IT support staff requirements and deliver services faster and more efficiently.

As new and disruptive technologies take over enterprise IT strategies, the obvious attention is towards information security – the increasing complexities, costs and skills required to manage security.

Importance of information security has increased multifold in the last many years due to proliferation of cyber crime, information being more distributed and legislations becoming more stringent. Information security is a mission critical initiative that has taken Board level cognizance.

Increasing cost and complexity of IT and growing threat landscape has made it difficult for organizations to manage security considerations on their own. These companies are turning towards outsourcing their security to third party experts, namely Managed Security Services Providers (MSSP).

Managed Security Services Market

Convergence of factors such as skill pressures, evolving and increasing threat landscape and compliance challenges is helping grow the Managed Security Services (MSS) market. IDC pegs the MSS market in APAC to be at USD 4 billion by 2015 growing in the next few years at a CAGR of about 20%.
As market continuously evolves and grows so are the services offered by MSSPs. Today service providers can manage day-to-day security tasks, secure and manage devices as well as provide analysis that can help organizations take better business decisions.

For small and mid sized organizations the managed model is a compelling proposition. The large capital expenditure (CAPEX) required to implement and manage the complex security environment of today is mitigated with this model.

Factors Driving Adoption of MSS

As threat landscape continues to evolve and get more and more sophisticated, economic pressures keep mounting and management of security becomes more complex and arduous, there is more pressure to improve efficiency, lower costs and adhere to stringent regulatory and compliance requirements.

Organizations are facing the following challenges that are factors driving increasing adoption of managed security services model:

**Evolving threat scenario**
Attacks on a company’s network is now motivated by financial gains, theft to intellectual property, malicious intent to defame the company or the brand, etc. These attacks are now more sophisticated than ever and require robust security framework, technologies and tools, management and monitoring and analysis of threat evolution.

**Lack of core competencies**
Managing security today requires constant monitoring, vigilant and committed security staff, complex analysis of every change in the network, etc. which may not be core competency of most user organizations.

**Proliferation of mobile devices**
Number of end points have exponentially increased over the years and employees are now encouraged to use devices of their choice with BYOD strategies being adopted by organizations. This puts a lot of pressure on security staff to manage and maintain security at increased number of devices, and ensure security and integrity of data that flows across all these devices.

**Increase in mobile workforce**
With increasing acceptance of mobile workforce and telecommuting at organizations today, the network has increased in size and area. As access to corporate networks increases so does the need to secure data that flows to these remote points.

**Increasing cost of security tools**
Cost of managing security has increased exponentially with increased technologies that go into security an organizations network and data, increasing cost of staffing, etc.

Benefits of Managed Security Services

Managed security services providers help to mitigate the risk and liability of managing security. Organizations are reaping multiple benefits from partnering with these experts. Some of the benefits and business advantages are:

**Reduced Cost**
This is one of the biggest advantages for organizations that outsource their security services to a third party service provider. MSSPs offer economies of scale by spreading cost of people and infrastructure across multiple clients.

**Infrastructure**
Infrastructure offered by MSSPs is specialized and multi locational – security operating centers (SOCs). These SOCs are manned by highly trained and skilled security experts, are state-of-the-art with best technologies implemented to ensure high levels of security for clients.

**Expertise**
MSSPs have the ability to attract, hire and motivate highly skilled security experts by offering continuous training, challenging work environment, career advancement, and myriad other opportunities. Organizations can benefit by having access to highly trained and motivated security experts.

**Adherence to Compliance**
Regulatory and compliance requirements are daunting on organizations to adhere to. For one it is the understanding of the complexity in the legal requirements. Then constantly tweaking solutions to adhere to it. Since MSSPs core focus is security for clients, they offer comprehensive knowledge of legal requirements and industry standards.

**Effectiveness and Performance**
Through state-of-the-art SOCs, MSSPs are able to provide 24x7 support, monitoring and management of security for organizations. They are able to deliver uninterrupted service and faster response to incidents as well as determine validate threats based on relevancy and reduce time spent on false alarms. Thus MSSPs are able to offer higher effectiveness and performance on security for organizations.

Risks Associated

Every coin has two sides. While benefits and options for outsourcing security services are various, they are not all void of risks associated to them. These risks are exacerbated due
to the critical nature of security for organizations.

To avoid risks associated with outsourcing security services to a third party service provider and to understand them better, organizations should be able to answer the following:

- Do you have critical and sensitive information that you do not want to relinquish control to a third party?
- Does the third party security services provider have agreements that will make them liable for critical parameters such as confidentiality, integrity, availability and loss of critical and sensitive data?
- Is there a back up to the data being stored at the third party provider? Is there a back up plan for if the service provider fails or goes out of business?
- Is the service provider going to be the bottleneck in your business by being the single point of failure? Is there a balanced view and plan for the same?

Answering and planning for these will help mitigate risks associated with outsourcing an organizations security services to a third party service provider.

It will be interesting to know some of the challenges that you face in managing security in your IT environment. Do share with us.
About Netmagic Solutions (An NTT Communications Company)

Netmagic, an NTT Communications company, is India’s leading Managed Hosting and Cloud Service Provider, with 8 carrier-neutral, state-of-the-art datacenters across the country. Established in 1998, Netmagic has been a pioneer in the Indian IT Infrastructure services space as it was the first to launch services such as cloud computing, managed security, Disaster Recovery-as-a-Service and software-defined storage. An IT Infrastructure Partner to more than 1400 enterprises globally, Netmagic, also delivers Remote Infrastructure Management services to NTT Communications’ customers across Americas, Europe and Asia-Pacific region. Netmagic is the recipient of several industry accolades and was recently chosen by India’s CIO community as the best service provider of Datacenter Managed Services and Cloud services, at the CIO Choice 2015 Awards. NTT Communications has subsidiaries and offices in 43 countries / regions, with over 21,600 employees worldwide. It had total operating revenues of 1230 billion JPY for year ending March 31, 2014 and has infrastructure worldwide, including leading global tier-1 IP network, the Arcstar Universal One™ VPN network reaching 196 countries/regions, and 130 secure datacenters.

NTT Communications is a part of NTT Corporation, Japan – one of world’s largest telecommunications companies and ranked 53 on Fortune Global 500 list (2014).

For further details please log into www.netmagicsolutions.com | Twitter: @netmagic | LinkedIn: @Netmagic Solutions

About NTT Communications Corporation

NTT Communications provides consultancy, architecture, security and cloud services to optimize the information and communications technology (ICT) environments of enterprises. These offerings are backed by the company’s worldwide infrastructure, including leading global tier-1 IP network, Arcstar Universal One™ VPN network reaching 196 countries/regions, and over 150 secure data centers. NTT Communications’ solutions leverage the global resources of NTT Group companies including Dimension Data, NTT DOCOMO and NTT DATA.