ARTICLE

The importance of an MSSP in a time of crisis

By Rishikesh Kamat
Vice President - Products & Services
NTT Global Data Centers and
Cloud Infrastructure, India
(erstwhile NTT-Netmagic)

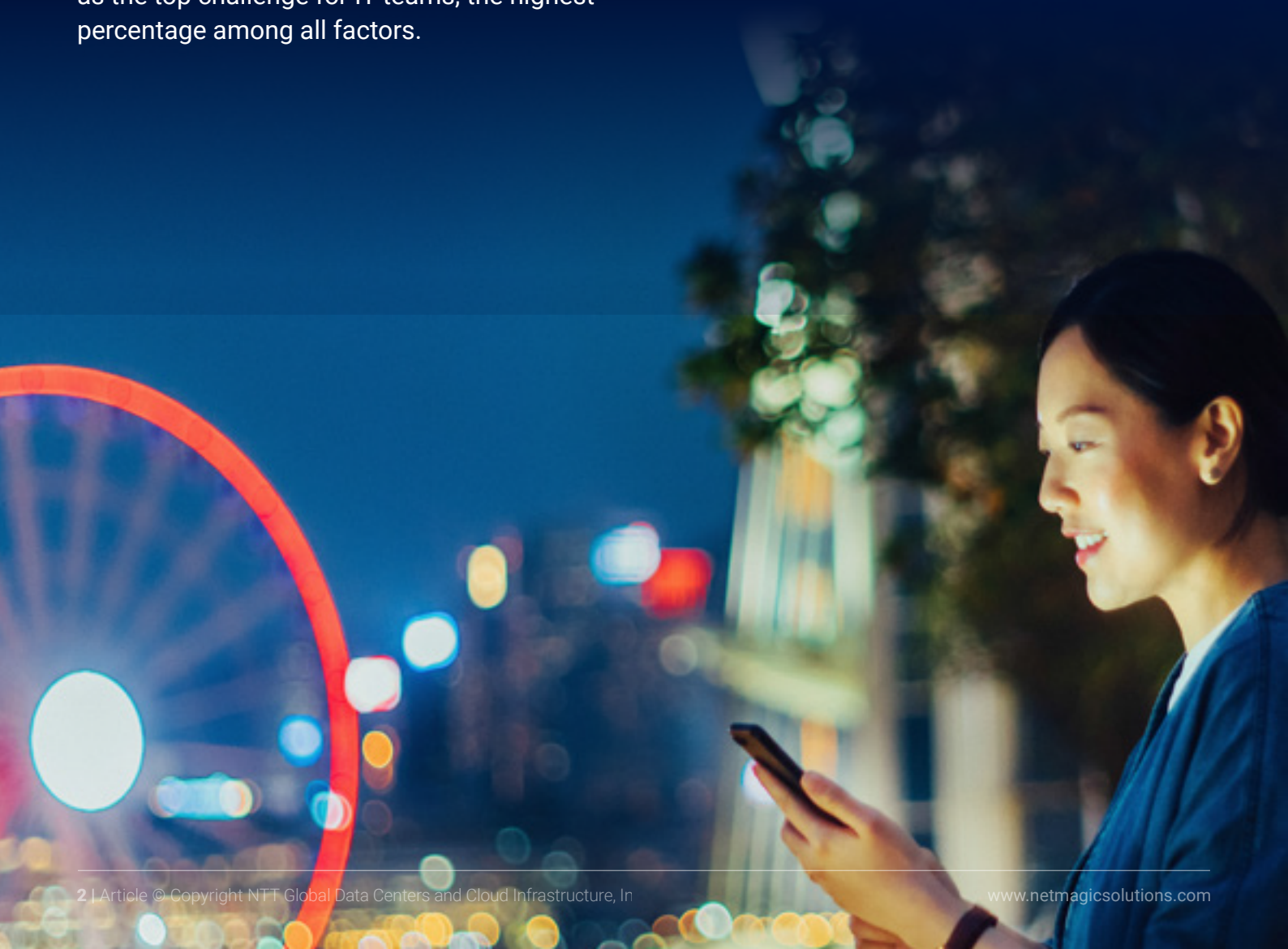
Even as organizations start transitioning to a work from home environment, the risks from remote workers poses a huge security risk. All employees do not have the same security infrastructure at home, which leaves them and the organization vulnerable to hackers. The International Information Systems Security Certification Consortium, (ICS)2, estimates that 23% of organizations have seen an increase in cybersecurity incidents since they have asked their employees to transition to remote work.

Managing a proactive security stance is challenging, and even more so, in a time of crisis such as Covid 19. A NTT 2020 Global Managed Services Report, states that as remote working becomes the preferred mode for working, 'reducing security risks' has been cited as the top challenge for IT teams, the highest percentage among all factors.

A constantly changing threat landscape makes it even more tough, and an organization's inhouse team is often overwhelmed enough to lose focus on the basics.

In times like these, Managed Security Services Providers (MSSPs) can be of great help. MSSPs offer a portfolio of services such as managed unified threat management services, intrusion detection services, managed SIEM services, compliance management, penetration testing services, vulnerability testing services and disaster recovery services.

Lets look at some of the key benefits of outsourcing information security requirements to an MSSP:



Sustained and constant monitoring of threats

MSSPs typically have access to thousands of customer networks and invest significantly in creating the best infrastructure and hiring of the best skilled resources. MSSPs can also create test environments for testing out if the infrastructure can handle global attacks. If enterprises were to do this on their own, the investment in manpower and infrastructure can be prohibitive in nature. MSSPs can also best equipped to identify the root cause of attacks and try to predict and prevent future attacks. In the current scenario, when networks and bandwidth is being overwhelmed by remote working, MSSPs can use their proven infrastructure to ensure secure access to employees. MSSPs can also evaluate and implement new security models to account for policy changes with respect to employees working from home. Through automated tools, MSSPs can also give a visibility of assets and their security gaps, especially when accessed remotely. Solutions suggested by MSSPs can be used for improving the organization's security posture.

Access to talent

Cyber security skill sets are always in demand, and most organizations do not have the capability to attract good talent. As MSSPs promise a good career and exposure to the latest technology trends equipped with best available infrastructure, they have the ability to attract the best possible talent, which in turn helps in warding off attacks. MSSPs also can retain talent in a far better manner as they can give them periodic training according to the latest available market trends.

Being compliant

Typically, organizations face a lot of challenges in keeping their data compliant in tune with industry regulations. For example, it could be the Payment Card Industry Data Security Standard (PCI DSS) or the Health Insurance Portability and Accountability Act (HIPAA) or Sarbanes-Oxley (SOX). Partnering with a MSSP can help in being compliant with the latest industry regulations.

Lower total cost of ownership

MSSPs can reduce the cost of securing infrastructure at a significantly lower cost as their cost of infrastructure and personnel is shared over multiple clients. More importantly, enterprises do not have to pay upfront for investing in capital expenditure, and can pay using a pay-per-month model. This results in substantial reduction in costs as clients do not have to invest in buying infrastructure or invest in hiring trained professionals for managing their infrastructure.

Access to best practices

With exposure to multiple clients and a constantly evolving competitive market, MSSPs keep on upgrading their skill sets and frameworks. For organizations whose core focus is not enterprise security, this can turn out to be extremely challenging. MSSPs can help organizations be at par with industry best practices and proactive security techniques such as analytics and behaviour-based detection to

predict, detect and prevent breaches. This is extremely critical in the current phase where advanced attacks have increased exponentially.

In summary, the Covid 19 crisis can be utilized by firms as an opportunity to improve their security posture by evaluating MSSPs to handle specific parts or their enterprise security.