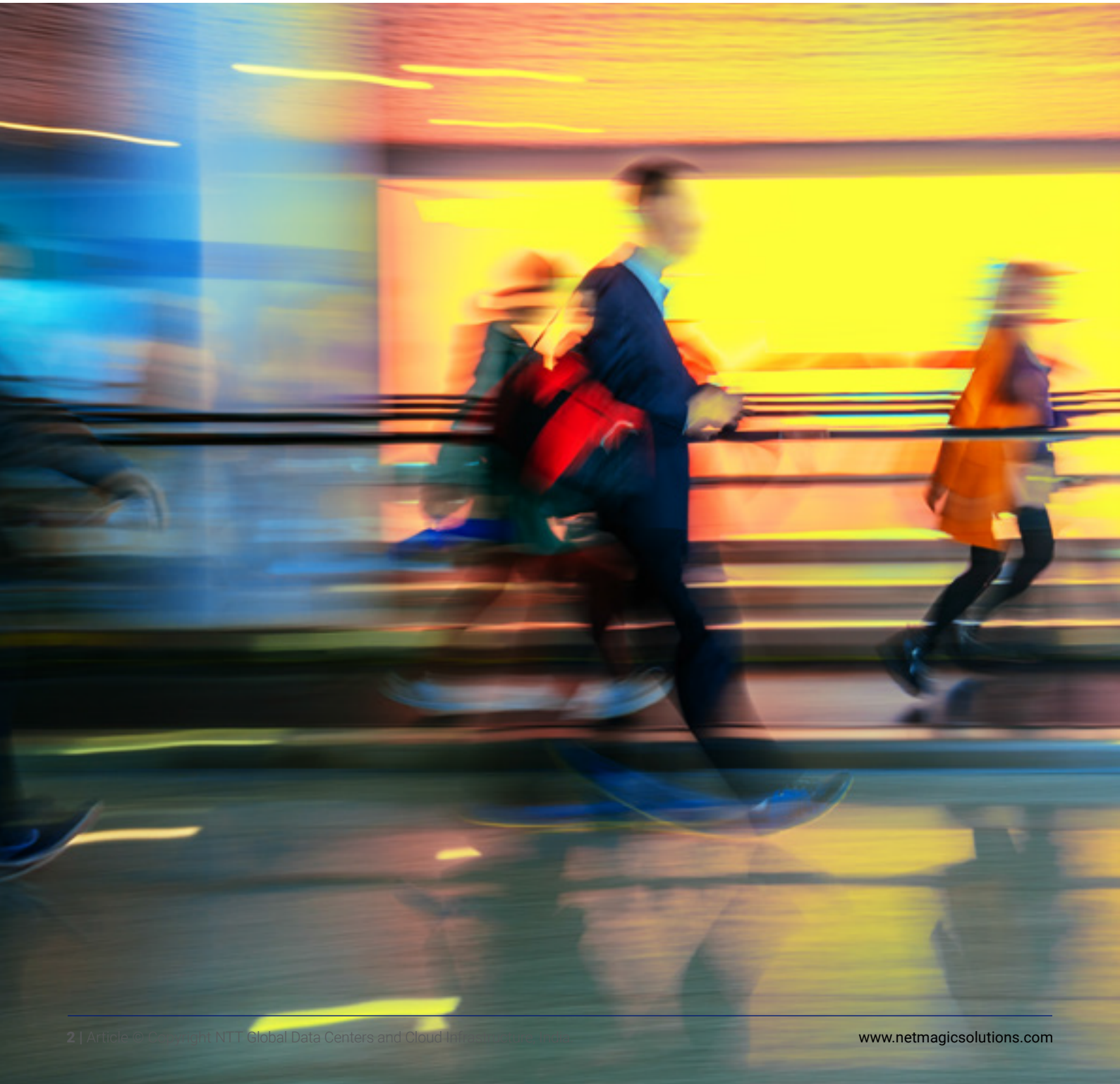
ARTICLE

Best practices in Business Continuity Planning: Now and for the future

Disasters are a common phenomena, and every organisation must have adequate plans and processes to ensure sustained business continuity

Every year, disasters - both manmade and natural, disrupt several lives. This year, the global pandemic, Coronavirus has completely altered the way organizations function -- forcing many organizations to bring about a change in the way they function. If one looks at the extensive damage caused by disasters, it reaffirms the need to have a comprehensive disaster recovery or business continuity policy in place.

We recommend the following best practices for ensuring sustained business continuity in the eventuality of any disaster:



Documenting the DR Policy

The business continuity plan must be drafted according to the risks, and the processes that needs to be followed in the event of a disaster. For example, the plan or process should clearly detail out what employees must do in the event of a disaster, and the maximum timeframe by which critical IT services will be delivered. It is also equally important to identify critical systems and take an inventory of the key applications. At the same time, organisations must document and have in place a list of external contacts such as bankers, IT consultants and utility personnel. As the coronavirus incident has taught us, organizations who had a well documented business continuity were the ones who could bounce back immediately.

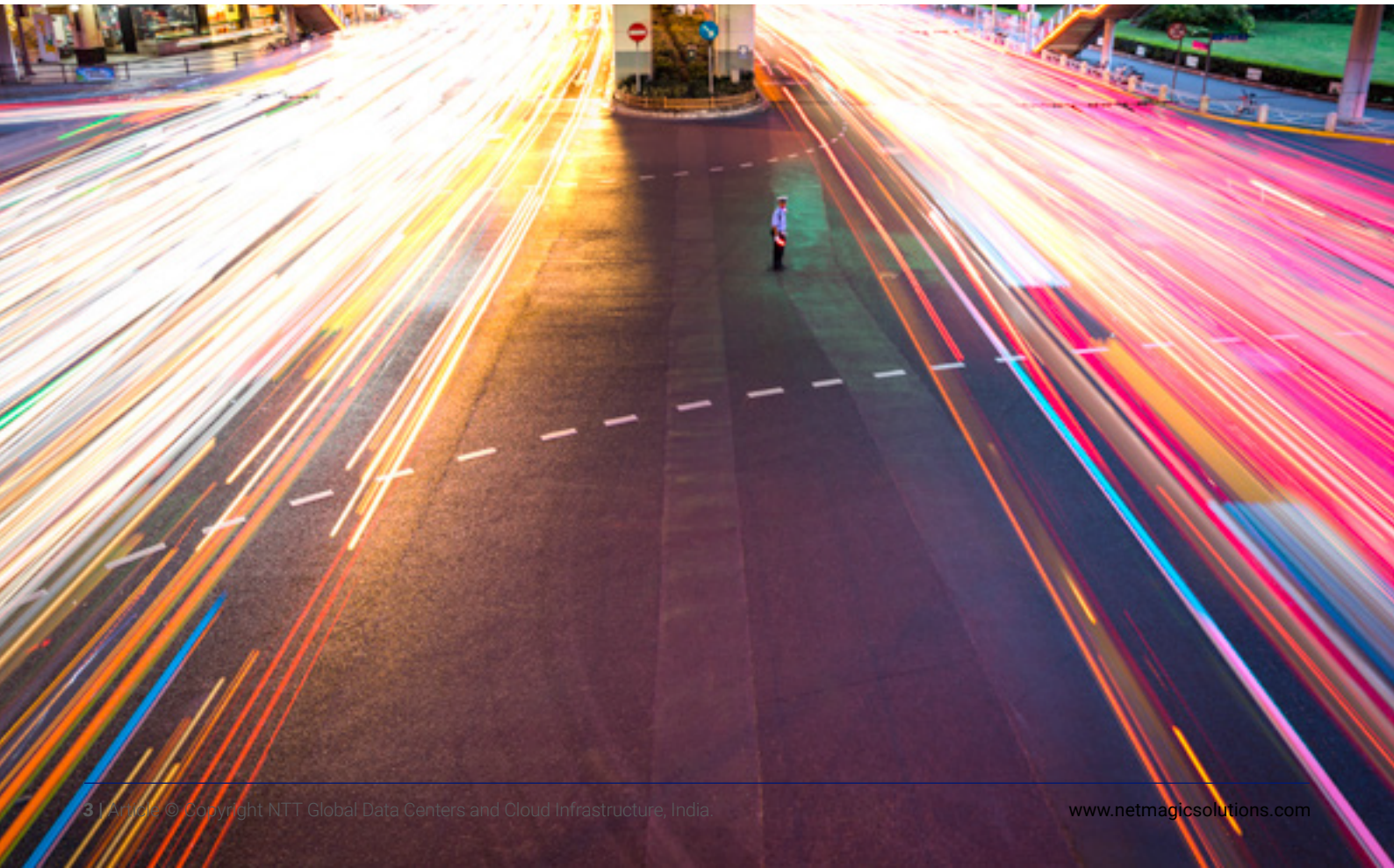
Determine your recovery options

As every organisation is unique, it must accordingly assess the risks and formulate a comprehensive comprehensive business continuity plan. The business continuity plan must be designed or created depending on the business that the organisation belongs to. For example, in the case of a bank or stock exchange, any downtime, even if it occurs for a few minutes, can cause losses in millions. For each organisation, it is important to define the approach to implement the required resilience so that the principles of incident prevention, detection, response, recovery and restoration are put in place.

Hence, depending on the business that an organisation belongs to, it must determine its recovery options. In DR or business continuity parlance, two terms - RTO and RPO are important. Recovery Point Objective (RPO) refers to the maximum acceptable data loss in terms of time, and Recovery Time Objective (RTO) denotes the amount of time between an outage and the restoration of operations. By selecting the right RPO and RTO according to business guidelines and requirements, one can select the right DR options and recovery technologies.

Communicate clearly with internal and external stakeholders

In a crisis, it is important to be proactive and communicate in detail about every possible information. For example, in the current crisis, it is imperative that organisations send detailed information via emails or WhatsApp groups to communicate the various ways by which they can operate smoothly from their home. In addition to a detailed list of FAQs on company policies, organisations must also appraise employees with respect to paid or sick leave options, insurance coverage and access to software tools to work from home. In addition, for clients, it is important to have a transparent and open communication with respect to availability of staff.



Prepare, prepare and prepare

Most disasters catch organisations by surprise. This is why organisations must mandatorily and regularly conduct DR drills. While many organisations have the customary DR drill, wherein employees perform the drill in a standard manner, they can fail as disasters are never the same. For example, during this crisis, many organisations realised that they did not the requisite VPN licenses for many employees. Many employees who were situated in tier II or tier III cities suffered from bandwidth issues. Hence, a business continuity plan must be subjected to multiple tests involving different scenarios to find out if there are any issues that will impact the success of the plan. This helps in preparing a more realistic assessment of different situations, which in turn can help in soliciting the required responses from different teams. By regularly conducting DR tests or drills, organisations can assess and analyse the business impact and progressively close all gaps, if they arise.

Keep in mind security risks

Disasters often leave the door open for security risks. As recent incidents have shown, there has been an increase in phishing attacks and threat actors have duly taken advantage of the panic to specifically create malware. Ransomware attacks are also common during a time of crisis, as systems are most vulnerable. At this time, it is important to review existing security policies and check endpoint security of devices. This is because as more remote workers work from their home, the security risks too increase as many home networks lack the common security mechanisms such as firewalls, antivirus software or backup tools. This increases the risk of malware spreading its way from individual devices to corporate networks.

Adopt a DR in the cloud option

If not already done, one must consider going in for a cloud-based business continuity plan. A cloud-based DR plan enables companies to quickly speed up the recovery time. The cloud option also enables companies to automatically provide access to services from any part in the world. For example, companies can empower their remote workers by delivering access to virtual desktops or critical applications. Moreover, with the elastic capability of the cloud, organisations can scale up their IT infrastructure in the cloud to meet increasing remote worker demands, as the coronavirus incident has demonstrated.