Why IT Resiliency Should Drive Your Post-COVID-19 Business Continuity Strategy

by **Gopalakrishnan Ramamoorthy (Gopal Ram)**

Lead - CBO Agile Computing, Cloud and Edge CoE

Abstract

Digital enterprises around the world are focused on managing the impact of the COVID-19 pandemic and looking at new best practices to help ensure business resiliency -- now and during any future disruptive events.

You can break resiliency into two pieces: Business resilience requires people and processes in order to maintain continuous business operations in the event of disruptions and data center outages. IT resilience involves people, process and technology to maintain availability of business applications. IT resilience is the heart of digital business and essential to run core business operations, including business resiliency and disaster recovery.

The Role of IT Resiliency in Ensuring Business Continuity

IT resiliency begins with the enterprise IT operations team. The team plays a vital role in maintaining uptime of the business applications in your on-premises data centers and public clouds as well as managing multiple resources including servers, storage systems, networks, load balancers, middleware, firewalls, applications and databases. The IT operations team is also responsible for ensuring availability during crises scenarios and needs to be standing by to enable various options for enterprises. As an example, during the COVID-19 lockdown, the IT ops team should be able to support the requirement for employees to work from home. However, IT operations do become more challenging when you add this complex requirement on top of day-to-day business IT operations and security compliance.

The Financial Impact of Downtime

Downtime can be caused by service unavailability of internal or external critical applications from cyberware or ransomware attacks; malfunction of hardware, software, or the network; natural disasters; human error; power outages — leading to significant impact to the business including lost revenue and loss of productivity, cost of recovery, competitor encroachment as well as intangible costs like erosion of brand reputation[1].

- In 2017 a large airline carrier had a major power failure during the holiday weekend, resulting in flight cancellations for more than its 75,000 passengers. This outage cost the company about $135 million.[1]
- Due to catastrophic IT issues, another airline failure resulted in cancellation of its 2,300 flights, causing delayed flight operations and negatively impacting many thousands of passengers as well as the brand.[2]
- During 2018, an Australian bank paid $7.4 million in compensation for an IT outage, according to its annual report.[3]
- When the Baltimore ransomware attack occurred in May 2019, the city's government computer systems were infected with aggressive ransomware called RobbinHood, which encrypted hard drive data to prevent access. This attack cost the city government approximately $18 million in damages.[4]

- In March of 2019, a Nordic metals firm was affected by ransomware attack called LockerGoga that shut down its global operations. This left their 35,000 employees around the world unable to work, resulting in a loss of productivity.[5]

Five Recommendations for an Effective IT Resiliency Strategy

The previous examples show that even pre-COVID-19, a proactive business continuity and resiliency strategy is a business imperative required to enable digital business, build robust resiliency into the infrastructure, and reduce downtime and associated costs.

Here are five approaches to build a robust IT resiliency strategy.

1. Use AI Powered Tools for Anomaly Detection

In a typical monitoring system, it is required to define static rules for thresholds. The thresholds ideally should be defined based on understanding of the respective system/application, since monitoring metric values differs from system to system. A value of the metric which is considered normal on Monday morning, for example, could be too high if observed on Sunday afternoon. Such occurrences of non-normalcy of metrics easily get missed from detection and alerts with typical monitoring solutions. Operation teams often manually view the historical metrics values and infer whether the metric value is normal or not and decide to investigate the problem if the value is deemed not normal. It is not possible to manually determine normalcy for every metric value for the entire infrastructure. It becomes increasingly difficult to do this with an ever-increasing infrastructure and the dynamic and agile nature of many components. Next-generation artificial intelligence (AI) operations provide a BAU (business-as-usual) dashboard, anomaly detection, predictive monitoring and metric co-relation features to help your IT operations team spot any abnormal behaviors and execute required actions, which brings self-healing capability and improves resiliency of your systems.

Example: A large North American retail giant looking to enhance customer experience by significantly reducing mean time to repair (MTTR) from the previous 120 mins and increase their IT efficiency by applying automation throughout their processes. A comprehensive blueprint makes AIOps solution context-aware of the 24 peak-season critical applications. Not only was "zero downtime" achieved but hundreds of tickets were auto resolved. The biggest benefit was a 30-minute reduction of MTTR for super-critical incidents and helped to maintain 100 percent availability of mission-critical applications.[6]

2. Follow an Immutable Approach

Immutable infrastructure is an approach to managing services and software deployments on IT resources wherein components are replaced rather than changed. An application or services is effectively redeployed each time any change occurs. If a change to a specification is required, an entirely new set of infrastructure is provisioned based on the updated requirements, and the previous infrastructure is taken out of service as it is then rendered obsolete. The growing use of containers are further contributing to the use of immutable infrastructure. Key benefits of adopting an immutable architecture approach includes the ability to easily switch to a previous, error-free version of the old image. Every change to the infrastructure can be executed through infrastructure as code. This immutable approach is leveraged in container-based environments, which offers multiple application deployment strategies and easy workload portability.

Example: A leading US bank deployed container orchestration platform deployment, which helps ensure faster time to market for their mobile and digital banking applications but also provides resiliency for business applications. The container platform helped to reduce downtime and faster rollback to the previous version as required, which created greater resiliency and availability.

3. Go with Self-Healing IT Infrastructure

At the same time, IT systems must expect failures and have a plan to be ready for them with a fast, effective recovery response. Best practices that can be included while building the strategy are the use of circuit breaker patterns, queue-based, load-leveling patterns, predictive analytics, infrastructure (as code with an immutable architecture) can help to build a fault-tolerant, resilient system that can survive gracefully.

Example: A leading European steel producer is currently on a digital transformation journey focused on innovation, customer focus, and value chain excellence at its core. The company has a complex IT landscape with a broad range of technologies in the areas of enterprise resource planning (ERP) and manufacturing execution system (MES) systems, data and reporting, planning and scheduling, and others. Within four months of implementing an IT resilient and self-healing solution, the company is handling 83% of its incidents and requests autonomously, and the customer has started reaping benefits such as faster turnaround times (98% reduction in lead time to fulfill requests) and elimination of manual errors.[7]

4. Bring in Disaster Recovery Automation

Disaster recovery (DR) automation enables seamless and successful DR drills for critical business applications and recovery of the applications at the DR target site with a single click. DR automation technology uses these industry metrics to calculate the resiliency factor during disaster recovery:

- Recovery time objective (RTO) – The duration of time and service level within which a business process must be restored after the disruption in order to avoid a break in business continuity.
- Recovery point objective (RPO) – The maximum tolerable period in which data might be lost.

DR automation solutions not only reduce SME dependencies during DR drills but also boost the confidence of the enterprise and provide comprehensive, real-time visibility into recovery readiness.

Example: Recently, one of the world's largest airlines had several outages of their critical applications. Their current DR recovery solution did not meet their business SLAs. The company's leadership team recognized that the existing, untested DR position left them at the risk of negative business impacts, which requires an RTO of two hours for critical applications. In addition, their applications have complex architecture with heterogeneous IT infrastructure landscape. The efforts to conduct DR drills and recovery was also very high and SME-dependent. Using automation, the airline was able to streamline the DR lifecycle to automate and simplify DR drills and meet the defined RTO/RPO for their business-critical applications. Plus, the solution was enabled with end-to-end DR management and reporting. The benefit of this automated approach to the airline was to improve DR predictability, increase the frequency of DR drills, and reduce the manual intervention required during such drills.

5. Apply Modern Practices for Data Protection and Recoverability

One of biggest threats for any enterprise is ransomware attacks, which are not even detected until weeks after the initial intrusion. Traditional solutions fail to detect such events and it can take many hours to recover and restore the system, which impacts the business. It is important to understand the location of backup systems. Regardless of multiple locations, it is a business imperative to simplify the operations with a consolidated unified view of the backup systems with rapid recovery options. Consider adopting next-generation data protection solutions that enable:

- RPOs reduced to minutes
- Complete automation for instant mass restore at any point of time along with best-in- class space efficiency
- Support for instant data backup for production, test and dev, compliance, security and analytics
- The use of immutable techniques, a robust defense strategy against ransomware, and minimized downtime using Machine Learning-driven detection and instant recovery

Example: A global bio-pharmaceutical company was running their backup and recovery operations with a legacy backup solution, which had a very complex environment. Maintaining and recovery of the backup infrastructure was a time-consuming challenge, failing to meet business requirements. The company implemented a modernized data protection solution with scale-out architecture and a single dashboard to manage the entire hybrid landscape (across on-premise and cloud) that provided protection from ransomware attacks. The benefits included simplified backup infrastructure and operations with instant recovery.

Summary

Now that the world has experienced the reality and the impact of a global disruption, it is clear that embracing a robust IT resiliency strategy is imperative for organizations to survive and thrive in any environment. It also requires leadership to ensure that business and IT resiliency strategies are continuously aligned to create value. As such, business continuity and resiliency must remain a top priority to ensure success -- right now and in the future.

Reference:

1 https://www.itnews.com.au/news/it-outage-to-cost-british-airways-135m-465278

2 https://www.zdnet.com/article/the-astonishing-hidden-and-personal-costs-of-it-downtime-and-how-predictive-analytics-might-help/

3 https://www.afr.com/technology/nabs-payments-systems-outage-cost-it-millions-in-compensation-20181116-h17ysd

4 https://foxbaltimore.com/news/local/estimated-at-least-18-million-needed-to-restore-city-accounts-in-ransomware-attack

5 https://www.bbc.com/news/business-48661152

6 https://insights.btoes.com/2019-award-finalist-spotlight-digitate-tcs-finalist-in-the-operational-excellence-in-banking-capital-markets-insurance-category-0

7 https://www.tcs.com/tcs-leader-in-cognitive-self-healing-it-infrastructure-management-services-nelsonhall

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

Experience certainty.

IT Services
Business Solutions
Consulting

TCS Design Services **I** M **I** 03 **I** 20