Disaster Recovery – Why being prepared is non-negotiable for modern businesses

By **Sachin Bhardwaj,** Director Marketing & Business Development, eHosting DataFort

Integrity of data is a critical concern for an enterprise. Information systems are a core functional asset of modern businesses andthe consequences of losing access to these systems or having their security undermined can have catastrophic consequences. From downtime and financial cost to loss of reputation and breached confidentiality, the services of Disaster Recovery companies can effectively mitigate anentire gamut of risks.

The ubiquitous use of technology and, in particular, information systems has revolutionized the way a modern business conducts its operations. While the upside of information technology has been gamechanging, the central role it occupies in processes can create its own concerns and vulnerabilities. Be it manufacturing or sales, process control or e-Commerce, the constant reliance on sharing and utilization of data can result in complete procedural paralysis, in the event that an IT system is undermined. Losses accrued can be both long or short term, and escalate into negative implications that impact the entire business in a matter of seconds.

According to a recent study, conducted by the University of Texas, an overwhelming 94% of companies suffering from a catastrophic data loss do not survive. Of these, 43% never reopen and 51% close within two years of the incident. A recent Gartner report further underscores the risks within an SME context – stating that 7 out of 10 small firms cease operations within a year of major data loss or IT disruption.

Data Recovery Services Providers address the concerns that such catastrophic consequences to the data integrity and information systems of an enterprise being compromised generate. As with every major international business hub, Disaster Recovery in Dubai and UAE has also matured into an industry that services enterprises in their quest to maximizing operational benefits while containing vulnerabilities.

Disaster Recovery helps mitigate a range of negative scenarios

Reasons for data integrity and information system related disasters can be manifold. Ranging from errors and accidents to malicious attacks.

- System Malfunction due to Software or Hardware errors and disruption in processes and systems due to technological malfunction is one of the most common sources of data loss and downtime. As powerful as our modern solutions are, they are not without their vulnerabilities.
- Human Error is another common reason for catastrophic data loss. From risk generating practices to accidental physical damage to infrastructure, human error driven vulnerabilities are always a possibility.
- Cyber Attacks and Malware have become an ever escalating aspect of risk in the modern day. Several recent Ransomware attacks have helped undermine the susceptibility of modern information systems to malicious attack. It can be tempting for small and medium enterprises to assume that such risks are limited to larger organizations, however recent patterns in cyber-crime have made such presumptions moot.
- Natural Disasters constitute perhaps the most uncontrollable cause of IT disasters. Extreme weather, earthquakes, large forest fires and floods are only some disaster scenarios that a business can be exposed to, depending on geography and location.

Clearly, it is nearly impossible for an organization to completely negate the possibility of an IT system and Data driven calamity. The sensible and proactive approach, for a modern enterprise, is to prepare effectively for the worst case scenario, rather than ignoring the consequences.

Elements that constitute effective Disaster Recovery Services

The services of a competent Disaster Recovery Company can help tremendously in allowing businesses the leeway to focus on core activities while concerns around worst case scenarios are addressed by the experts.

A Disaster Recovery Company's services typically entail the following:

- Service Level Agreements that address Recovery Point and Recovery Time Objectives.
- Creating a Disaster Recovery Runbook template.
- Assessment and diagnosis across the entire system and applications employed by the business.
- Conducting frequent DR drills and addressing issues that are identified.
- Liaising with external vendors and third parties for continued support of deployed technologies, within an acceptable range of metrics.