Disaster Recovery

As computer hardware and associated infrastructure have evolved High Availability subsystems have considerably reduced the probability of a disastrous situation occurring. It however remains prudent that all enterprises retain a high degree of Disaster Recovery readiness. A comprehensive Disaster Recovery Plan should at the very minimum address the risk of data corruption of loss caused by:

1. Accidental or malicious actions of staff.
2. Programmatic data corruption.
3. Failure of storage and replication sub-systems.
4. Virus, Denial of Service (DoS) and other system shutdown caused by security compromise.
5. Hardware and storage asset confiscation by law enforcement agencies under court order.