Chapter XII
Networking Technologies for Business Continuity

CHAPTER OVERVIEW

Continuous computing technologies explored in previous chapters, in many cases, are located on different locations. However, they depend on each other and are bound to data communication and networking technologies that are used in order to ensure data transfers. Therefore, the data communications technologies are crucial in ensuring continuous computing each time when computing devices and users are located in different locations. Chapter XII provides some explanations on them and their role in business continuity.

NETWORK INFRASTRUCTURE AND NETWORK DOWNTIME

Networking infrastructure is a prerequisite for any kind of e-business in networked economy. It consists of several data communications and computer network technologies that are implemented in order to come up with appropriate data communications—computer network platform. Computer network infrastructure is very important from business continuity perspective since any disconnection failure that occurs on it can cause data unavailability.

As shown in Figure 12.1, these technologies make the third layer of an information system that enables continuous computing.

They include technologies such as communication devices, communication media, communication protocols, network operating systems, networking protocols,
data protection and security standards. Network cards, modems, cable modems, DSL modems, routers, bridges, switches, hubs, firewalls, and so forth, are used to connect computers within local area networks, wide area networks, virtual private networks, campus networks, metropolitan networks. Several communication media, guided and non-guided, such as leased lines, ISDN, ATM, frame-relay, wireless communications devices and protocols, satellite communications, and so forth, are used in order to establish several types of computer networks. These networks are in turn basis for networked enterprises, e-business, e-government and e-economy. Hunter (2008) noted that recent Internet outages in the Middle-East bring customary boom in business continuity.

In addition to data communication hardware and software glitches and failures, another threat with regard to business continuity is in network attacks. Network attacks today can come in the form of competitive espionage, disgruntled ex-employees, hackers, crackers, other forms of outsiders willing to use our servers to store music, movies, pornography, pirated software and so on.

In modern Internet era, in what is called “networked business,” the network security in an organization that operates in such a kind of environment is a business continuity problem. A famous saying, “A chain is only as strong as its weakest link” applies as a rule in modern e-business.

Network downtime caused by security attacks is costing large enterprises more than $30 million a year, according to a recent study by Infonetics Research.

Figure 12.1. Continuous computing layers: The role of networking infrastructure (Layer 3)


[www.igi-global.com/chapter/impact-assessment-of-policies-and-practices-for-agile-software-process-improvement/204248?camid=4v1a](www.igi-global.com/chapter/impact-assessment-of-policies-and-practices-for-agile-software-process-improvement/204248?camid=4v1a)