51

Introduction

As more and more businesses are operating in an e-business environment, they are under pressure to “keep their business in business” continuously. It is particularly important to ensure this for data/information availability, because continuous data access and availability are sought by employees, current and prospective customers, suppliers, and other stakeholders. Therefore, most businesses today seek for an information system infrastructure that is running 24/7/365, ensuring that data and applications are continuously available.

Information technologies have brought new opportunities for businesses in their efforts to increase their profits, reduce the costs, enhance the quality of products and services, improve relations with customers, and ease data access. However, at the same time, IT-related problems have produced new business risks as well. Unavailable data, stolen or lost computers, hardware glitches, server operating system crashes, application software errors, damaged backup tapes, broken data communication connections, a destroyed computer center due to several types of natural disasters, hackers’ activities, and power outages are just some situations that may cause interruptions in business computing and affect the whole business.

The nature and characteristics of IT-associated risks have dramatically changed over two recent decades. While some 20–30 years ago an IT-related problem on a computer center's mainframe was viewed only as a “technical” problem causing a delay in, for instance, payroll system schedule, today similar problem may affect financial results and a corporation’s competitive position or even bring the whole business into a halt. Unlike those times when most businesses operated on a “five-days-a-week” and “9 am–5 pm” basis, currently, it is common for most businesses to run on a 24/7/365 schedule. Hence, the role of business computing is becoming more important than ever with a special emphasis on becoming “continuous computing.” It is no longer just about faster data processing, management of data, support for decision making, but rather about “keeping business in business.” Business technology—a buzzword coined by Forrester (2007)—represents one of the major shifts in the way
people think about computers in IT history. According to Forrester, business technology is based on two key ideas: (1) IT risks are business risks and (2) IT opportunities are now business opportunities.

“Business continuity” (BC) or “business continuance” is a general term that emphasizes the ability of a business to continue with its operations and services even if some sort of failure or disaster on its computing platform occurs. Therefore, BC is rather to be defined as an ultimate objective of modern business with regard to capability of its information system to provide both continuous computing and business resilience. Modern business seeks for an information infrastructure that is going to be always on with zero downtime or highly available with near-zero-downtime. Symantec’s Small and Medium Business (SMB) Disaster Preparedness Survey (2011) revealed that disasters can have a significant financial impact on SMBs. At the time of this survey, the median cost of downtime for an SMB was $12,500 per day. Aberdeen Group found recently (Csaplar, 2012) that between June 2010 and February 2012, the cost per hour of downtime increased on average by 65%. In February 2010, the average cost per hour of downtime was reported to be about $100,000.

51.2 Business Continuity Defined and Impact on Practice

51.2.1 Business Continuity Defined

The concept of BC reflects the dependence of modern business on its information system infrastructure. If an enterprise’s information system is up with mission-critical applications running and providing services to end users, business is said to be “in business.” When an application server running a critical e-business application goes down for any reason, business simply becomes “out of business.” Therefore, the process of addressing, mitigating, and managing the IT risks has become one of the major issues in organizational IT management.

Today’s IT-related threats/risks that may cause system unavailability and hence affect the business can be classified into the following major categories:

- Technical glitches and/or hardware component failures within the IT infrastructure: processors, memory chips, mainboards, hard disks, disk controllers, tapes and tape drives, network cards, fans, power supply unit.
- Physical damage to/thefts of IT centers, servers, client computers, mobile devices, or communication/networking devices.
- Operating system crashes: crashes of server operating systems that run enterprise servers and make server applications available to end users.
- Internal threats such as intentional malicious or retaliation acts of disgruntled IT staff and other insiders including former employees, operational errors, careless behavior of users and system administrators, human errors such as accidental or deliberate deletion of system and configuration files, unskilled operations, mistakes by well-intentioned users, and hazardous activities including sabotage, strikes, epidemic situations, and vandalism.
- External threats that range from individuals hacking the Internet sites on curiosity basis to organized criminals and professionals working for industrial espionage purposes. These include Internet-based security threats such as viruses, malware, botnets, malicious code, Denial-of-Service or Distributed Denial-of-Service (DoS or DDOS) attacks, spam, intrusion attacks, phishing, and moles.
- File or process-based problems such as corrupted configuration files, broken processes or programs, and file system corruption.
- Application software defects: bugs in programs, badly integrated applications, user interventions on desktop computers, corrupted files, etc.
- LAN/WAN/Internet disconnections, hardware failures on data communication devices, software problems on network protocols, Domain Controllers, gateways, Domain Name Server (DNS) servers, Transmission Control Protocol/Internet Protocol (TCP/IP) settings, etc.
Business Continuity

- Loss or leaving of key IT personnel: bad decisions on IT staffing and retention, particularly with regard to system administrators.
- Natural threats such as fire, lightning strike, flood, earthquake, storm, hurricane, tornado, snow, and wind.

These threats are shown in Figure 51.1.

In addition to several types of hardware failures, physical damages on computer systems, and natural threats, a number of threats coming from inside and outside of computer centers may cause system unavailability. These threats are in most cases addressed to enterprise servers given their role in modern business computing. Particularly, external threats require more attention as the servers are, by default, as follows:

- Accessible, available, tend to be always on, and running on continuous basis. Therefore, they are subject to continuous attacks from external attackers. Server-oriented attacks are much more expected than attacks to personal systems.
- Having several configuration files that can be misused (e.g., /etc/passwd file, /etc/hosts file, allow/deny access files on Unix/Linux).

![Figure 51.1 Major IT-related threats and risks.](image-url)
• Having a number of services set on the “on” mode (open, active) after installation that opens the door for possible attacks.

• Storing business-critical applications and end user data to be accessed on remote basis, instead of keeping data on desktop/portable computers.

Addressing these threats leads to the process of mitigating (reducing) downtime situations and achieving continuous computing. Operating environment that facilitates continuous computing is a hardware–software platform that encompasses several technologies that are necessary for efficient and effective business-critical applications. Its characteristics will be discussed at a more detailed level in later sections.

Sumner (2009) unveiled the results of a study of top security threats perceived by organizations with over 500 employees as (1) deliberate software attacks, (2) technical software failures or errors, (3) acts of human error or failure, (4) deliberate acts of espionage or trespass, and (5) deliberate acts of sabotage or vandalism. ITIC Report (2009) unveiled the fact that server hardware and server operating system reliability have improved vastly since the 1980s, 1990s, and even in just the last 2–3 years. While technical bugs still exist, the number, frequency, and severity have declined significantly. This report underscores the fact that with few exceptions, common human error poses a bigger threat to server hardware and server operating system reliability than technical glitches. Adeshiyan et al. (2010) stated that traditional high-availability and disaster recovery solutions require proprietary hardware, complex configurations, application-specific logic, highly skilled personnel, and a rigorous and lengthy testing process. They provide some guidelines on how virtualization can be used in order to achieve high availability (HA) and disaster recovery.

The term “continuous computing” will be defined in the following way:

• By computing, we refer to an information system implemented by using information and communication technologies.

• By continuous, we refer to the ability of an information system to have both applications and data available on continuous basis for end users, customers, suppliers, and other stakeholders.

When an application server running business-critical or any other business application is not operational, it is said to be “down” or “off.” The time in which it does not operate is called “downtime.” Downtime refers to a period of time that a computing infrastructure component is not functioning, in most cases as a result of some system failure such as hardware component failures, operating system crashes, application software malfunctioning, regular maintenance, and so on.

Downtime can be planned or expected, and unplanned or unexpected (undesired). Planned downtime is a result of planned operations due to several administrative tasks or reasons for shutting application and/or operating system down. On the server side, it includes administrative tasks on servers, server operating systems, applications, LANs, and the WAN. Planned downtime is scheduled, usually duration-fixed, due to planned operations made mainly by system administrators such as regular data backups, hardware maintenance and upgrade, operating system upgrades and updates, application updates, and periodic events such as different types of hardware and software testing processes. Unplanned downtime is unanticipated, duration-variable downtime of a computer system due to several types of natural disasters, power outages, infrastructure failures, hardware or software failures, human errors, lack of proper skills, etc. Recent advances in information technologies allow several administrative operations on servers, both hardware and software interventions, without halting the system down.

The opposite is uptime. Uptime is a measure of the time a computer system such as a server has been “up,” running and providing services. It has three main dimensions that reflect the capabilities of a server platform to be available, reliable, and scalable.

• High availability refers to the ability of a server operating environment to provide end users an efficient access to data, applications, and services for a high percentage of uptime while minimizing both planned and unplanned downtime. It is the ability of a system (server, operating system,
application, network) to continue with its operation even in cases of hardware/software failures and/or disasters. IDC (2010) pointed out that HA is critical to building a strong BC strategy. HA is the foundation of all BC strategies.

- **High reliability** refers to the ability of a server operating environment to minimize (reduce) the occurrence of system failures (both hardware and software related) including some fault-tolerance capabilities. Reliability goals are achieved by using standard redundant components and advanced fault-tolerant solutions (hardware, systems software, application software).

- **High scalability** refers to the ability of a server operating environment of scaling up and out. Servers can be scaled up by adding more processors, RAM, etc., while scaling out means additional computers and forming cluster or grid configurations.

The term “high availability” is associated with high system/application uptime, which is measured in terms of “nines” (e.g., 99.999%). The more nines that represent availability ratio of a specific server, the higher level of availability is provided by that operating platform. According to IDC, HA systems are defined as having 99% or more uptime. IDC (2006, 2009) defined a set of different availability scenarios according to availability ratio, annual downtime, and user tolerance to downtime with regard to several continuous computing technologies that are available today (Table 51.1).

Table 51.2 correlates the number of nines to calendar time equivalents.

All these uptime dimensions can be identified and investigated for several components independently such as server hardware, operating system, application servers, network infrastructure, the whole server environment, or whole information system. Ideas International (IDEAS, www.ideasinternational.com) provides detailed analyses of most widely used server operating platforms with regard to several uptime dimensions.

### 51.2.2 Impact on Practice

In August 1995, Datamation quoted the results of a survey of 400 large companies that unveiled that “… downtime costs a company $1400 per minute, on average. Based on these figures, 43 hours of downtime per year would cost $3.6 million. One hour of downtime per year amounts to $84,000 per year” (Datamation, 1995). Recounting a situation in which eBay’s auction site experienced a serious problem,
Managing and Securing the IT Infrastructure and Systems

A study by Nielsen Media Research and NetRatings Inc. (Dembeck, 1999) describes how the average time spent per person at Yahoo's auction site increased to 18 min on Friday from 7 min on Thursday—the night eBay's site crashed. The number of people using Yahoo's site also skyrocketed to 135,000 on Saturday from 62,000 on Thursday. But the number of users fell to 90,000 on Monday. Financial losses to eBay were estimated at $3–$5 million. Starting from the mid-1990s, there have been several stories and studies on the costs of downtime.

Hiles (2004) estimated that IS downtime put direct losses on brokerage operations at $4.5 million per hour, banking industry $2.1 million per hour, and e-commerce operations $113,000. Fortune 500 companies would have average losses of about $96,000 per hour due to the IS downtime. Nolan and McFarlan (2005) quoted that an attack on Amazon.com would cost the company $600,000 an hour in revenue; they also claimed that if Cisco's systems were down for a day, the company would lose $70 million in revenues.

Another event, primarily based on the lack of scalability, occurred in October 2007 when the Beijing 2008 Olympic Committee started the process of online ticket reservation. The server infrastructure went down immediately after the online reservations and sales were activated. The website for online ticket sales received a couple of million page views with an average of 200,000 ticket requests filed every minute. The system was designed to handle a maximum of one million visits per hour and a maximum of 150,000 ticket requests per minute (Computerworld, 2007).

Martin (2011) cited the results of the study by Emerson Network Power and the Ponemon Institute, which revealed that the average data center downtime event costs $505,500 with the average incident lasting 90 min. Every minute the data center remains down, a company is effectively losing $5600. The study took statistics from 41 U.S. data centers in a range of industries, including financial institutions, health-care companies, and collocation providers.

CA Report (2011) provides the results of an independent research study to explore companies' experiences of IT downtime in which 2000 organizations across North America and Europe were surveyed on how they are affected by IT downtime. The key findings include the following:

- Organizations are collectively losing more than 127 million person hours each year through IT downtime and data recovery with each company losing 545 person hours a year.
- Each business suffers an average of 14 h of downtime per year.
- Organizations lose an average of nine additional hours per year to data recovery time.
- 87% of businesses indicated that failure to recover data would be damaging to the business, and 23% said this would be disastrous.

Fryer (2011) explored some characteristics of several downtime incidents that happened in 2011 such as Verizon's LTE mobile data network outage that lasted several days and Alaska Airlines's server outage in March 2011, which resulted in the cancellation of 15% of the scheduled flights. Neverfail Report (2011) revealed results from a survey of 1473 SME and Enterprise IT professionals in the United States regarding their disaster recovery plans and practices. According to this report,

- Twenty-three percent of respondents have had an IT outage for more than one full business day.
- Hardware and software problems cause most of the IT outages (43% or respondents), while others reported power and datacenter outages (35%), natural disasters (8%), human error (6%), and others (8%).

Forrester conducted a joint research study with Disaster Recovery Journal on most common causes of downtime. In their report (Forrester, 2011, p. 2), they pointed out “Most disasters are still caused by mundane events. That headlining disaster that you're watching out for most likely won't be what causes your downtime—instead, it'll be a backhoe operator at the construction site next door who accidently severs your power or network lines.”

All these studies and reports demonstrated the importance of downtime costs and emphasized the need for implementing more advanced availability, scalability, and reliability solutions that may help...
in enhancing BC. In addition to technology solutions, several methodologies, methods, and research approaches have been developed over the last decade in order to address these topics in an academic way, not only from technology perspective. In the section that follows, some of these approaches are briefly elaborated.

### 51.3 Information Architectures: The Downtime Points

Businesses operating in an e-business environment are in most cases run by different forms of business-critical applications. These applications are installed on application servers and accessed by end users over network, often designed or based on the client–server architecture (c/s). Such an architecture consists of one or more servers hosting business-critical applications and a number of clients accessing them. Depending on the server infrastructure’s availability, reliability, and scalability, the whole business operates with more or less downtime that, in turn, has more or less impact on its financial performance.

Several models of information architectures have been identified over the last four decades depending mainly on the evolution of hardware and software.

Turban et al. (2005) defined the notion of “information technology architecture” as a high-level map or plan of the information assets in an organization, which guides current operations and is a blueprint for future directions. Jonkers et al. (2006) defined architecture as “structure with a vision,” which provides an integrated view of the system being designed and studied. They build their definition on top of a commonly used definition by the IEEE Standard 1471–2000. Versteeg and Bouwman (2006) defined the main elements of a business architecture as business domains within the new paradigm of relations between business strategy and information technologies. Goethals et al. (2006) argued that enterprises are living things, and therefore, they constantly need to be (re)architected in order to achieve the necessary agility, alignment, and integration. Balabko and Wegmann (2006) applied the concepts of system inquiry (systems philosophy, systems theory, systems methodology, and systems application) in the context of an enterprise architecture. Lump et al. (2008) provided an overview of the state-of-the-art architectures for continuous availability concepts as HA clustering on distributed platforms and on the mainframe. Bhatt et al. (2010) considered IT infrastructure as “enabler of organizational responsiveness and competitive advantage.”

Today’s information systems are mainly based on the three major types of information architecture: legacy–mainframe environment, several models of client–server architectures, and cloud computing-based platforms.

While mostly considered obsolete, the mainframe-based information architecture has been still in use with the redefined role of today’s mainframe configurations as servers or hosts within the c/s architecture. Moreover, today’s mainframes are used as servers in a cloud-based computing environment. They are known for their HA ratios, e.g., IBM’s z systems (www.ibm.com) with the latest versions bringing the redundant array of independent memory (RAIM) technology as a fault-tolerant RAM.

Client–server architectures consist of servers and clients (desktop computers and portable/mobile devices) with applications being installed and running on server computers. Server’s side of such architecture is called “business server” or “enterprise server” or, in a broader sense, “server operating environment.” It consists of server hardware, server operating system, application servers, and standard server-based and advanced server technologies (also known as “serverware”) that are used to enhance key server platform features such as reliability, availability, and scalability. A hybrid architecture is used as well: a combination of mainframe (legacy) platform with newly implemented “thick” or “thin” client–server applications installed on servers.

Enterprise servers running server operating systems are expected to provide an operating environment that must meet much more rigorous requirements than a desktop operating system such as Windows XP or Windows 7 can provide. System uptime that is used as a measure of the availability is one of the most critical requirements.

© 2014 by Taylor & Francis Group, LLC
No matter which of the c/s models is implemented, some most commonly used layers of the client–server architecture can be identified as follows:

- **Client layer**—a layer that is represented by a client application (“thick” or “thin,” depending on the type of client–server architecture that is implemented). Each user, from any business unit, department, or business process, uses appropriate client application or web browser over this client layer.
- **Networking layer**—a layer that consists of a number of different data communication devices, data communication media, hardware and software communication protocols, and applications implemented for data communications.
- **Server operating platform layer**—a layer consisting of one or more servers (data, application, web, messaging, firewall, etc.) accompanied by server operating systems and integrated serverware solutions.
- **Data storage layer**—a layer that contains several data storage, data backup, and recovery solutions intended to be used for data storage.

Several modifications of standard c/s architecture are in use today as well in the forms of newly created computing paradigms or models such as web-enabled legacy systems, utility/on-demand computing, software-as-a-service, web-based software agents and services, subscription computing, grid computing, clustering, ubiquitous or pervasive computing, and cloud computing. They are implemented primarily in order to reduce the costs and enhance uptime.

A number of problems that cause downtime may occur within all types of information architectures such as hardware glitches on server components, operating system crashes, network interface card malfunctions, WAN/Internet disconnections, application bugs, system or network administrator’s errors, or natural disasters that hit main computer center or cloud computing provider’s site (Figures 51.2 and 51.3).

**FIGURE 51.2** Downtime points in a client–server architecture.
All these situations may cause unavailability of applications and hence result in a business going “out of business.” Therefore, information technologies today play a crucial role by providing several so-called continuous computing technologies that may reduce downtime or enhance the levels of uptime. In all cases, no matter which type of information architecture is used, the server side of the client–server model consisting of one or more application servers plays a crucial role in ensuring the availability of business-critical applications. The downtime points are considered critical in implementing continuous computing solutions for enhancing BC.

Today, cloud computing as a concept tends to replace almost all aforementioned concepts and becomes a platform of choice for many businesses today. Forrester predicts that the global cloud computing market will grow from $40.7 billion in 2011 to more than $241 billion in 2020 (Dignan, 2011). However, the role of servers and server operating environment remains almost the same as business-critical applications are again run by server computers, with the only difference being in the fact that these servers reside within the boundaries of cloud computing provider but not in business’s computer center.

Cloud outages such as those of Amazon and Google from April 2011 (Maitland, 2011) showed that even within “by default” highly available infrastructures such as the cloud providers’ data centers downtime is still possible and requires attention. In the Amazon’s case, huge demand of Lady Gaga fans for the discounted album caused Amazon’s servers going down for several hours. In addition, more than 10 h of unavailability of Amazon’s servers caused unavailability of some popular websites such as Quora and Reddit. It turned out that these couple of cloud outages could have an impact on the attractiveness of the whole concept of cloud computing (Sisario, 2011).
Cloud requires the same care, skills, and sophisticated management as other areas of IT (Fogarty, 2011). Peiris, Sharma, and Balachandran (2010) developed a Cloud Computing Tipping Point (C2TP) model, which is intended to be used by organizations when deciding between embracing cloud offerings and enhancing their investments in on-premise IT capabilities. Within the model, they list BC and higher uptime as primary attributes for this model. AppNeta revealed recently (Thibodean, 2011) that the overall industry yearly average of uptime for all the cloud service providers monitored by AppNeta is 99.9948%, which is equal to 273 min or 4.6 h of unavailability per year. The best providers were at 99.9994% or 3 min of unavailability a year.

In both standard and web-based client/server and cloud-based architectures, a number of possible problems or critical points can be identified with regard to possible downtime problems:

- Client data-access-related problems on the client PC or client computing devices: hardware, operating system, client applications
- Network infrastructure problems: LAN/WAN/Internet disconnections from servers
- Server operating platform: crashes of server hardware and server operating system
- Data storage: hard disk crash, corrupted file system, magnetic tape broken

As said before, servers can be affected by several types of hardware glitches and failures, system software crashes, application software bugs, hackers’ malicious acts, system administrators’ mistakes, and natural disasters like floods, fires, earthquakes, hurricanes, or terrorist attacks. Therefore, the process of addressing and managing the IT-related threats has become an important part of managing information resources in any organization. In addition to standard hardware/software failures, some human-related activities can cause system downtime as well.

### 51.4 Framework for Business Continuity Management

By using Churchman’s approach in defining the systemic model (Churchman, 1968, 1971) already applied in explaining information systems for e-business continuance (Bajgoric, 2006), the objective of a continuous computing platform in an organization can be defined as achieving the BC or business resilience. Several information technologies can be applied in the form of continuous computing technologies. This approach leads to identifying the “always-on” enterprise information system that can be defined as an information system with a 100% uptime/zero downtime.

Following Churchman’s systemic model, the objective of an “always-on” enterprise information system in an organization can be identified as providing the highest availability, reliability, and scalability ratios for achieving the BC or business resilience. In other words, this refers to the following: continuous data processing with continuous data access and delivery, multiplatform data access, on-time IT services, and better decisions through better data access. Such an information system employs numerous continuous computing information technologies and builds and integrates several components that are aimed at enhancing availability, reliability, and scalability ratios.

A conceptual model used here to illustrate the concepts of BC and continuous computing technologies is given in Figure 51.4.

Continuous computing technologies are considered to be major BC drivers. These technologies include several IT-based solutions that are implemented in order to enhance continuous computing (uptime) ratios such as availability, reliability, and scalability and include the following 10 major technologies:

1. Enterprise servers (server hardware)
2. Server operating systems (server operating environments)
3. Serverware solutions in the form of bundled, in most cases, vendor-specific solutions installed as a set of extensions to standard server operating system
4. Application servers

© 2014 by Taylor & Francis Group, LLC
51-11

Business Continuity

5. Server-based fault-tolerance and disaster-tolerance technologies
6. Server clustering
7. Data storage and backup solutions
8. Advanced storage technologies such as mirroring, snapshot, data vaulting
9. Networking and security technologies
10. System administration knowledge and skills

All these technologies are identified as the main building blocks of an always-on enterprise information system. They are represented within the three continuous computing layers as seen in Figure 51.5. The continuous computing technologies can be implemented within the following three layers:

1. Layer 1—Server and server operating environment
2. Layer 2—Data storage, data backup, and recovery technologies
3. Layer 3—Data communications and security technologies within a networking infrastructure

The first group mainly includes so-called preemptive technologies—standard and specific information technologies and human skills that aim at “preempting” or preventing downtime and keeping system uptime as higher as possible. The second group of continuous computing technologies relate to those solutions that help in recovering from failures and disaster that caused system and application downtime (post-failure). The third group consists of data communications, networking, and security technologies that are used to connect business units and its information system’s subsystems and to keep them connected and secure in order to have continuous and secure data access and data exchange. A more detailed depiction of these technologies is given in Figure 51.6 in a revised form of so-called Onion model (Bajgoric, 2010).
As can be seen in Figure 51.6, the main technologies that are used to provide HA ratios can be classified into the following categories:

- Server-based technologies
- Server operating systems, enhanced by serverware solutions
- Data storage and backup technologies
- Data communications and networking technologies
- Fault-tolerance and disaster-tolerance technologies
- Redundant units and/or devices such as power supplies and fans, hard disks, network, interface cards, routers, and other communication devices
- Facilities such as UPS units, dual power feeds or generators, and air-conditioning units
- Advanced technologies, such as virtualization, mirroring, snap-shooting, clustering, and data vaulting
- Security and protection technologies
- Predictive system-monitoring capabilities that are aimed at eliminating failures before they occur

Server-based technologies include several types of hardware and software features that support HA technologies such as SMP, clustering, 64-bit computing, storage scalability, RAID and RAIM technologies, fault tolerance, hot spared disk, HA storage systems, online reconfiguration, grid containers, dynamic system domains, virtual machine managers, and hardware and software mirroring. In addition, server platform-based serverware suites include bundled servers, reloadable kernel and online upgrade features, crash-handling technologies, workload management, HA monitors, and Windows/UNIX integration.

Several server operating systems, both commercial proprietary and open source, provide additional HA features. For instance, HP’s HP-UX 11.0 server operating platform (http://www.hp.com) provides several HA features such as advanced sys_admin commands (e.g., fsck, lvcreate, make_recovery, check_recovery), Veritas’s VxFS JFS—Journaled File System, JFS snapshot, dynamic root disk, Bastille, Compartments, fine-grained privileges, role-based access control, and HP Serviceguard. JFS is a recommended file
system for high reliability, fast recovery, and online administrative operations. Recently developed new file system by Microsoft for its Windows Server operating system is named the “Resilient File System” (ReFS). It is built on the existing NTFS, enhanced by some additional resiliency features.

Fault-tolerant and disaster-tolerant systems include the following technologies: redundant units, data replication, hot sites, data vaulting, and disaster recovery sites. Some of these technologies overlap with data storage systems, which include standard tape backup technology, Storage Area Networks (SAN), Network Attached Storage (NAS), off-site data protection, Fibre Channel, iSCSI, Serial ATA, etc.

Security and protection technologies that are implemented on computer hardware (servers, desktops, laptops, non-PC computing devices), systems software (restricted use of system privileges, user accounts monitoring, etc.), application software, networking devices such as routers, switches, firewalls, control of network ports, protocols and services, and network applications are also part of unified continuous computing platform shown in Figure 51.6.

The ultimate goal of data communications technologies from BC perspective can be identified as staying connected with employees, customers, and suppliers and ensuring a set of communication technologies to support workforce during disastrous events that interrupt business. These technologies include unified communication technologies that integrate data, e-mail, voice, and video and collaboration

FIGURE 51.6 “Onion” model: unified continuous computing paradigm.
technologies supporting personal productivity software on portable devices, scheduling, web-based collaboration, and content sharing.

The management dimension of the systemic model presented in Figure 51.4 consists of two main aspects of BC management:

1. **Technical aspect** that encompasses system administration activities on operating system and networking levels. Two professional roles responsible for these activities are system and network administrators, respectively.

2. **Managerial aspect** that is characterized by organization-wide efforts to design and implement BC strategies, policies, and activities. BC manager is a person responsible for these tasks. He/she, however, has to work closely with the CIO who is responsible for the whole information technology environment.

System and network administration represent core activities of organizational BC efforts. Technical skills of system administrators or “super-users,” and their experience and several “tips and tricks” that they use in administering operating system platforms and computer networks are crucial in maintaining servers and networks up and running on always-on basis. This applies for both preemptive and post-failure operations and activities. Experienced and skilled system/network administrators can significantly improve the levels of system/network uptime while system/network is operational and reduce recovery time in case of system/application or network crashes. The fact that system administrator holds an all-powerful administrative account is a potential risk as well and must be addressed within the managerial scope of organizational BC management.

51.5 Research Issues and Future Directions

This section provides some insights on current works, research issues, and future research directions related to BC. Recent publications are selected and assessed within the following aspects:

- Terminology used
- Frameworks and methodologies
- Business impact
- BC and disaster recovery
- BC and related disciplines such as risk management, auditing, and supply chain management
- IT architectures related

51.5.1 Current Works and Research Issues

From historical perspective, business continuity as a concept has been treated extensively over the last 15–20 years. As already stated in Section 51.2, in the very beginning of the e-business era, Datamation (1995) emphasized the importance of minimizing system downtime. Herbane (2010) noted that business continuity management (BCM) has evolved since 1970s in response to the technical and operational risks that threaten an organization’s recovery from hazards and interruptions. Regarding the terminology, Broder and Tucker (2012) underlined that BC planning is defined in many different ways reflecting its author’s particular slant, background, or experience with the process. They make the difference between the meaning of continuity planning and of a continuity plan. Nollau (2009) introduced the term “enterprise business continuity” and argued that each company should have a functional plan that addresses all processes required to restore technology, an individual responsible for that plan, and a disaster response team at the ready. King (2003) introduced a term “Business Continuity Culture” and underscored the fact that “If you fail to plan, you will be planning to fail.” Kadam (2010) introduced the concept of personal BC management.

With regard to BCP frameworks, Botha and Von Solms (2004) proposed a cyclic approach to BC planning with each cycle concentrated on a specific BCP goal. Gibb and Buchanan (2006) defined a framework for
the design, implementation, and monitoring of a BC management program within an information strategy. They assign the CIO a key role in both promoting the philosophy of BCM and ensuring that information management incorporates effective plans, procedures, and policies to protect information assets. Gerber and Solms (2005) emphasized the need for a holistic approach that should include a carefully planned security policy, the use of technology, and well-trained staff. They proposed an integrated approach based on analyzing not only risks to tangible assets but also risks to information or intangible assets. Cerullo and Cerullo (2004, p. 71) stated that “… there is no single recommended plan for business continuity; instead, every organization needs to develop a comprehensive BCP based on its unique situation.”

Boehman (2009) presented a model for evaluating the performance of a BCM System according to BS 25999 standard. The model calculates the survivability ex-ante if the key performance indicator for the effectiveness exists. Lindstrom et al. (2010) noted that organizations rely too much on the checklists provided in existing BC standards. These checklists for predefined situations need to be created during the BCP process and kept updated in the following maintenance process. They proposed a multi-usable BC planning methodology based on using a staircase or capability maturity model. Herbane, Elliott, and Swartz (2004) examined the organizational antecedents of BCM and developed a conceptual approach to posit that BCM, in actively ensuring operational continuity, has a role in preserving competitive advantage.

Walker (2006) considered outsourcing options for BC. Bartel and Rutkowski (2006) proposed a fuzzy decision support system for IT service continuity (ITSC) management. They argued that ITSC management is typically part of a larger BCM program, which expands beyond IT to include all business services within an organization. Brenes et al. (2011) focused on assessing the impact of BC-related governance structures on family business performances. Avery Gomez (2011) underscored the fact that resilience and the continuity of business are factors that rely on sustainable ICT infrastructures. The author presented a model for alignment of BC and sustainable business processes with regard to ICT usage behavior and response readiness. Sapateiro et al. (2011) presented a model of a mobile collaborative tool that may help teams in managing critical computing infrastructures in organizations with regard to BC management.

As for the business impact, in addition to what was said in Section 51.2, several authors still emphasize the impacts of downtime on business. According to Stanton (2007, p. 18), “… it can take less than 60 seconds for a company’s reputation to be ruined and its business to be crippled. In just one minute, a server failure or hacker can knock out vital applications.” He underscored the saying “Fail to Plan, Plan to Fail.” Melton and Trahan (2009) argued that critical risks demand critical attention. Vatanasombut et al. (2008) noted that the proliferation of Internet has not only allowed businesses to offer their products and services through web-based applications but also undermined their ability to retain their customers. Ipe et al. (2010) stated that satisfying decision making in public health often stems from the unavailability of critical information from the surveillance environment. They explored the challenges specific to developing and institutionalizing an IT system for emergency preparedness.

Bertrand (2005) researched the relationships between BC and mission-critical applications. He emphasized the role of Replication Point Objective (RPO) and Replication Time Objective (RTO) in recovering from disasters and stressed the role of replication technologies in providing better RPO and RTO values. IDC (2010) pointed out that HA is critical to building a strong BC strategy meaning that HA is the foundation of all BC strategies. Forrester (2009) unveiled that almost 80% of respondents reported that their firms have had to provide proof of BC readiness.

Zobel (2011) defined an analytic approach in representing the relationship between two primary measures of disaster resilience: the initial impact of a disaster and the subsequent time to recovery. Singhal et al. (2010) presented a solution for optimal BC based on the IP SAN storage architecture for enterprise applications used for data management without burdening application server. In order to achieve zero RPO, they proposed introducing a staging server in addition to DR site with replication performances. Lewis and Pickren (2003) pointed out that disaster recovery is receiving increasing attention as firms grow more dependent on uninterrupted information system functioning. Turetken (2008) developed a decision model for locating redundant facilities (IT-backup facility location) within the activities of BC planning. Bielski (2008) stated that some think of BC as doing what is necessary to set up a “shadow”
organization that will take you from incident response through various phases of recovery. Omar et al. (2011) presented a framework for disaster recovery plan based on the Oracle’s DataGuard solution that includes remote site, data replication, and standby database.

Pitt and Goyal (2004) saw BCM as a tool for facilities management. They argued that both FM and BCP are important on strategic level and pointed out the need for the involvement of facilities manager in BC planning. Yeh (2005) identified the factors affecting continuity of cooperative electronic supply chain relationships with empirical case of the Taiwanese motor industry. Wu et al. (2004) identified continuity as the most important behavioral factor on business process integration in SCM. Hepenstal and Campbell (2007) provided some insights on transforming Intel’s worldwide Materials organization from crisis management and response to a more mature BC approach. According to these authors, the BC-oriented approach improved Intel’s ability to quickly recover from a supply chain outage and restoring supply to manufacturing and other operations. Craighead et al. (2007) considered BC issues within the supply chain mitigation capabilities and supply chain disruption severity. They proposed a multiple-source empirical research method and presented six propositions that relate the severity of supply chain disruptions. Tan and Takakuwa (2011) demonstrated how the computer-based simulation technique could be utilized in order to establish the BC plan for a factory. Blackhurst et al. (2011) provided a framework that can be used to assess the level of resiliency and a supply resiliency matrix that can be utilized to classify supply chains according to the level of resiliency realized. Kim and Cha (2012) presented the improved scenario-based security risk analysis method that can create SRA reports using threat scenario templates and manage security risk directly in information systems.

Wan (2009) argued that in current business-aligned IT operations, the continuity plan needs to be integrated with ITSC management if an organization is going to be able to manage fault realization and return to normal business operations. He proposed the framework based on using the IT service management portal and network system-monitoring tool. Winkler et al. (2010) focused on the relationships between BCM and business process modeling. They proposed a model-driven framework for BCM that integrates business process modeling and IT management. Kuhn and Sutton (2010) explored the alternative architectures for continuous auditing by focusing on identifying the strengths and weaknesses of each architectural form of ERP implementation.

According to IDC’s white paper (2009), by adopting industry best practices (e.g., ITIL, CobIT) and updating their IT infrastructure, companies can lower annual downtime by up to 85%, greatly reducing interruptions to daily data processing and access, supporting BC, and containing operational costs. Umar (2005) explored the role of several business servers in designing an IT infrastructure for “next-generation enterprises.” Butler and Gray (2006) underscored the question on how system reliability translates into reliable organizational performance. They identify the paradox of “relying on complex systems composed of unreliable components for reliable outcomes.” Adeshiyan et al. (2010) stated that traditional high-availability and disaster recovery solutions require proprietary hardware, complex configurations, application specific logic, highly skilled personnel, and a rigorous and lengthy testing process.

Williamson (2007) found that in BC planning, financial organizations are ahead of other types of businesses. Kadlec (2010) reported on the IT DR planning practices of 154 banks in the United States. Ardini and Morabito (2010) argued that the financial sector sees BC not only as a technical or risk management issue but also as a driver toward any discussion on mergers and acquisitions. Sharif and Irani (2010) emphasized HA, failover, and BC planning in maintaining high levels of performance and service availability of eGovernment services and infrastructure.

### 51.5.2 Summary of Recent Publications

Table 51.3 provides a summary of recent publications published over the last 10 years about BC, BC management, and related topics. They are listed with regard to research focus and main contribution.
<table>
<thead>
<tr>
<th>Article Year</th>
<th>Authors</th>
<th>Research Focus/Main Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003</td>
<td>Lewis and Pickren</td>
<td>Presented a technique that can be used to assess the relative risk for different causes of IT disruptions</td>
</tr>
<tr>
<td>2003</td>
<td>King</td>
<td>Introduced a term &quot;Business Continuity Culture.&quot; Underscored the fact “If you fail to plan, you will be planning to fail”</td>
</tr>
<tr>
<td>2004</td>
<td>Botha and Von Solms</td>
<td>Proposed a BCP methodology that is scalable for small and medium organizations. Developed a software prototype using this cyclic approach and applied it to a case study</td>
</tr>
<tr>
<td>2004</td>
<td>Herbane et al.</td>
<td>Examined the organizational antecedents of BCM and developed a conceptual approach to posit that BCM, in actively ensuring operational continuity, has a role in preserving competitive advantage</td>
</tr>
<tr>
<td>2004</td>
<td>Finch</td>
<td>Revealed that large companies’ exposure to risk increased by interorganizational networking and that having SMEs as partners in the SCM further increased the risk exposure</td>
</tr>
<tr>
<td>2004</td>
<td>Wu et al.</td>
<td>Identified continuity as the most important behavioral factor on business process integration in SCM</td>
</tr>
<tr>
<td>2004</td>
<td>Pitt and Goyal</td>
<td>Considered BCM as a tool for facilities management</td>
</tr>
<tr>
<td>2004</td>
<td>Cerullo and Cerullo</td>
<td>Provided guidelines for developing and improving a firm's BCP consisting of three components: a business impact analysis, a DCRP, and a training and testing component</td>
</tr>
<tr>
<td>2005</td>
<td>Bertrand</td>
<td>Estimated the relationships between BC and mission-critical applications. Emphasized the role of RPO and RTO in recovering from disasters and stressed the role of replication technologies</td>
</tr>
<tr>
<td>2005</td>
<td>Yeh</td>
<td>Identified the factors affecting continuity of cooperative electronic supply chain relationships with empirical case of the Taiwanese motor industry</td>
</tr>
<tr>
<td>2005</td>
<td>Gerber and Solms</td>
<td>Suggested the need for a holistic approach that should include a carefully planned security policy, the use of technology, and well-trained staff. The article indicated how information security requirements could be established</td>
</tr>
<tr>
<td>2005</td>
<td>Umar</td>
<td>Investigated the role of several business servers in designing an IT infrastructure for “next-generation enterprises”</td>
</tr>
<tr>
<td>2006</td>
<td>Walker</td>
<td>Considered outsourcing options for BC</td>
</tr>
<tr>
<td>2006</td>
<td>Bartel and Rutkowski</td>
<td>Argued that ITSC management is typically part of a larger BCM program, which expands beyond IT to include all business services. Proposed a fuzzy decision support system for ITSC management</td>
</tr>
<tr>
<td>2006</td>
<td>Butler and Gray</td>
<td>Underscored the question on how system reliability translates into reliable organizational performance. Identified the paradox of “relying on complex systems composed of unreliable components for reliable outcomes”</td>
</tr>
<tr>
<td>2006</td>
<td>Gibb and Buchanan</td>
<td>Defined a framework for the design, implementation, and monitoring of a BC management program within an information strategy</td>
</tr>
<tr>
<td>2007</td>
<td>Williamson</td>
<td>Found that in BC planning, financial organizations are ahead of other types of businesses</td>
</tr>
<tr>
<td>2007</td>
<td>Hepenstal and Campbell</td>
<td>Provided some insights on transforming Intel’s worldwide Materials organization from crisis management and response to a more mature BC approach</td>
</tr>
<tr>
<td>2007</td>
<td>Craighead et al.</td>
<td>Proposed a multiple-source empirical research method and presented six propositions that relate the severity of supply chain disruptions</td>
</tr>
<tr>
<td>2008</td>
<td>Vatanasombut et al.</td>
<td>Argued that the proliferation of Internet has not only allowed businesses to offer their products and services through web-based applications but also undermined their ability to retain their customers</td>
</tr>
<tr>
<td>2008</td>
<td>Bielski</td>
<td>Stated that some think of BC as doing what is necessary to set up a “shadow” organization that will take you from incident response through various phases of recovery</td>
</tr>
</tbody>
</table>

(continued)
### TABLE 51.3 (continued)  
Review of Literature Related to Business Continuity

<table>
<thead>
<tr>
<th>Article Year</th>
<th>Authors</th>
<th>Research Focus/Main Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008</td>
<td>Turetken</td>
<td>Developed a decision model for locating redundant facilities (IT-backup facility location) within the activities of BC planning</td>
</tr>
<tr>
<td>2008</td>
<td>Lump et al.</td>
<td>Investigated several aspects and relationships among HA, disaster recovery, and BC solutions</td>
</tr>
<tr>
<td>2009</td>
<td>Wan</td>
<td>Argued that in current business-aligned IT operations, the continuity plan needs to be integrated with ITSC management</td>
</tr>
<tr>
<td>2009</td>
<td>Boehman</td>
<td>Presented a model for evaluating the performance of a BCM System according to BS 25999 standard. The model calculates the survivability ex-ante if the key performance indicator for the effectiveness exists</td>
</tr>
<tr>
<td>2009</td>
<td>Nollau</td>
<td>Introduced the term &quot;enterprise business continuity&quot;</td>
</tr>
<tr>
<td>2010</td>
<td>Adeshiyan et al.</td>
<td>Stated that traditional high-availability and disaster recovery solutions require proprietary hardware, complex configurations, application-specific logic, highly skilled personnel, and a rigorous and lengthy testing process</td>
</tr>
<tr>
<td>2010</td>
<td>Ipe et al.</td>
<td>Stated that satisfying decision making in public health often stems from the unavailability of critical information from the surveillance environment. They explored the challenges specific to developing and institutionalizing an IT system for emergency preparedness</td>
</tr>
<tr>
<td>2010</td>
<td>Singhal et al.</td>
<td>Presented a solution for optimal BC based on the IP SAN storage architecture for enterprise applications used for data management without burdening application server</td>
</tr>
<tr>
<td>2010</td>
<td>Kuhn and Sutton</td>
<td>Explored the alternative architectures for continuous auditing by focusing on identifying the strengths and weaknesses of each architectural form of ERP implementation</td>
</tr>
<tr>
<td>2010</td>
<td>Tammineedi</td>
<td>Categorized the key BCM tasks into three phases of BC: pre-event preparation, event management, and post-event continuity. The Business Continuity Maturity Model of Virtual Corporation presented as a tool</td>
</tr>
<tr>
<td>2010</td>
<td>Lindstrom et al.</td>
<td>Proposed a multi-usable BC planning methodology based on using a staircase or capability maturity model</td>
</tr>
<tr>
<td>2010</td>
<td>Kadlec</td>
<td>Reported on the IT DR planning practices of 154 banks in the United States</td>
</tr>
<tr>
<td>2010</td>
<td>Arduini and Morabito</td>
<td>Argued that the financial sector sees BC not only as a technical or risk management issue but also as a driver toward any discussion on mergers and acquisitions. The BC approach should be a business-wide approach and not an IT-focused one</td>
</tr>
<tr>
<td>2010</td>
<td>Winkler et al.</td>
<td>Focused on the relationships between BCM and business process modeling. Proposed a model-driven framework for BCM that integrates business process modeling and IT management</td>
</tr>
<tr>
<td>2010</td>
<td>Kadam</td>
<td>Introduced the concept of personal BC management</td>
</tr>
<tr>
<td>2011</td>
<td>Tan and Takakuwa</td>
<td>Demonstrated how the computer-based simulation technique could be utilized in order to establish the BC plan for a factory</td>
</tr>
<tr>
<td>2011</td>
<td>Zobel</td>
<td>Presented an analytic approach in representing the relationship between two primary measures of disaster resilience: the initial impact of a disaster and the subsequent time to recovery</td>
</tr>
<tr>
<td>2011</td>
<td>Omar et al.</td>
<td>Presented a framework for disaster recovery plan based on the Oracle's DataGuard solution that includes remote site, data replication, and standby database</td>
</tr>
<tr>
<td>2011</td>
<td>Greening and Rutherford</td>
<td>Proposed a conceptual framework based on network theories to ensure BC in the context of a supply network disruption</td>
</tr>
<tr>
<td>2011</td>
<td>Brenes et al.</td>
<td>Focused on assessing the impact of BC-related governance structures on family business performances</td>
</tr>
<tr>
<td>2011</td>
<td>Avery Gomez</td>
<td>Presented a model for alignment of BC and sustainable business processes with regard to ICT usage behavior and response readiness</td>
</tr>
</tbody>
</table>
51.5.3 Future Research Directions

Future research directions with regard to BC can be identified around the following research topics:

- Integrating BC management, IT management, and organizational management
- Positioning BC as part of business risk management
- Exploring relations between BC management and disaster recovery management
- Developing and implementing advanced server technologies for enhancing servers’ availability, reliability, and scalability
- Developing frameworks for organization-wide implementation of BC
- Implementing several information technologies as BC drivers
- BC and IT/IS security
- BC and information resources management
- BC and system and network administration
- BC in cloud computing environment
- HRM dimensions of BC management: the roles of system and network administrators, BC managers, IT managers, CIOs, and CSOs
- Implementing BC within the compliance regulations, legislations, and standards on BCM

Given the fact that several terms and buzzwords related to BC have been introduced over the last decade, it would of interest to further explore and develop theoretical aspects and practical implications of those terms such as business continuity, business continuance, business resilience, always-on business, zero-latency business, always-available enterprise, and so on.

51.6 Conclusions

Modern business owes a lot to information technology. It is well known that information technologies provide numerous opportunities for businesses in their efforts to reduce the costs, increase the profits, enhance the quality of products and services, improve relations with customers, and cope with increasing competition. At the same time, modern businesses face several situations in which they may suffer due to some IT-related problems that cause lost data, data unavailability, or data exposed to competition. In addition, some businesses experienced so-called IT-based horror stories due to bad implementations of enterprise information systems.

With advances in e-business, the need for achieving “a near 100%” level of business computing availability was brought up yet again. Consequently, the term “business continuity management” was coined up and became a significant part of organizational information management. BCM has become an integral
part of both IT management and organizational management. It involves several measures (activities) that need to be implemented in order to achieve higher levels of the system/application availability, reliability, and scalability ratios. BC relies on several continuous computing technologies that provide an efficient and effective operating environment for continuous computing. Implementation of continuous computing technologies provides a platform for “keeping business in business.” Therefore, an enterprise information system should be managed from BC perspective in a way that this process includes both managerial and system administration activities related to managing the integration of BC drivers.

In this paper, an attempt was made to explore the concept of business continuity from both managerial and IT perspective. In addition, several illustrations of downtime costs are provided in order to demonstrate the importance of BC for modern business.

References


ITIC Report (2009), ITIC 2009 global server hardware and server OS reliability survey, Information Technology Intelligence Corp. (ITIC), July 2009


