Security has been a concern since the early days of computing, when a computer was isolated in a

room and a threat could be posed only by malicious insiders. The Pandora’s box1 of threats opened

wide once computers were able to communicate with one another. In an interconnected world, various

embodiments of malware can migrate easily from one system to another, cross national borders, and

infect systems all over the globe.

The security of computing and communication systems takes on a new urgency as society becomes

increasingly dependent on the information infrastructure. Nowadays, even the critical infrastructure

of a nation can be attacked by exploiting flaws in computer security. Malware, such as the Stuxnet

virus, targets industrial control systems controlled by software [81]. Recently, the term cyberwarfare

has entered the dictionary with the meaning “actions by a nation-state to penetrate another nation’s

computers or networks for the purposes of causing damage or disruption” [85].

A computer cloud is a target-rich environment for malicious individuals and criminal organizations.

It is thus no surprise that security is a major concern for existing users and for potential new users

of cloud computing services. In Section 3.10 we identified some of the security threats perceived by

cloud users; in Section 9.1 we elaborate on this topic. Some of these risks are shared with other systems

supporting network-centric computing and network-centric content, e.g., service-oriented architectures

(SOAs), grids, and Web-based services.

Cloud computing is an entirely new approach to computing based on a new technology. It is therefore

reasonable to expect that new methods to deal with some of the security threats will be developed,

whereas other perceived threats will prove to be exaggerated. Indeed, “early on in the life cycle of a

technology, there are many concerns about how this technology will be used . . . they represent a barrier

to the acceptance . . . over the time, however, the concerns fade, especially if the value proposition is

strong enough” [174].

The idea that moving to a cloud liberates an organization from many technical concerns related to

computer security and eliminates internal threats is accepted by some members of the IT community.

As we shall see throughout this chapter, this seems a rather na ve point of view, because outsourcing

computing to a cloud generates major new security and privacy concerns. Moreover, service-level

agreements do not provide adequate legal protection for cloud computer users, who are often left to

deal with events beyond their control.

One of the consequences of the breathtaking pace of development of information science and technology

is that standards, regulations, and laws governing the activities of organizations supporting the new

computing services, and in particular utility computing, have yet to be devised or adopted. As a result,

many issues related to privacy, security, and trust in cloud computing are far from settled. The pool of

resources of a cloud service provider can be dispersed over several countries or even several continents.

Since information can freely cross national borders there is a need for international regulations to be

adopted by the countries where data centers of cloud computing providers are located.