# Chapter 6.2
# E-Business Systems Security for Intelligent Enterprise

**Denis Trček**
*Jožef Stefan Institute, Ljubljana, Slovenia*

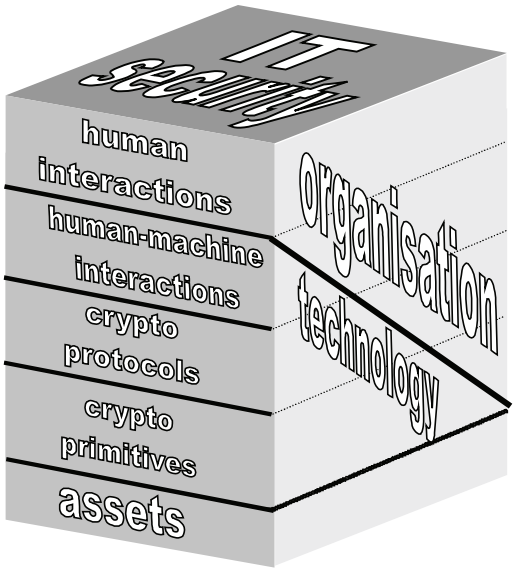
## ABSTRACT

*Security issues became a topic of research with the introduction of networked information systems in the early eighties. However, in the mid-nineties the proliferation of the Internet in the business area exposed security as one of key-factors for successful on-line business. The majority of efforts to provide security were focused on technology. However, it turned out during the last years that human factors play a central role. Therefore, this chapter gives a methodology for proper risk management that is concentrated on human factors management, but it starts with addressing classical, i.e. technology based issues. Afterwards, business dynamics is deployed to enable a quantitative approach for handling security of contemporary information systems. The whole methodology encompasses business intelligence and presents appropriate architecture for human resources management.*

## INTRODUCTION

The importance of computer based information systems (IS) was recognized decades ago, but fundamental changes started with the penetration of computer networks. When Porter was emphasizing the importance of information for gaining competitive advantage in the mid-eighties (Porter, 1985), some visionary authors recognized that the most promising potential for information management is actually hidden in computer communications (McFarlan, 1984). This was proved in the ’90s, when the electronic business era started. It became clear that computer communications technology has changed not only the nature of information systems, but business in general. Information technology (IT) turned out to be the main driving factor for business strategies (Kalakota, 1999). New business models emerged and reengineering of existing business processes became necessary. Concentration on internal business processes with emphasis on

*Figure 1. E-business systems security with focus on management of human factors*




products or services was no longer sufficient. The emphasis moved to the end of value chains, i.e., customers. Competitive advantage was achieved by linking competing chains through knowing and understanding customers. A deployment of highly sophisticated techniques enabled better fulfillment of customers needs (Sweiger, 1999). Successful external and internal data integration and management became essential for proper decision-making. Non-tangible outputs of business processes started to represent main parts of added value and IS were transformed into Web-based, customer centric information systems.

It is therefore obvious that security of information systems is getting a part of core business processes in every e-business environment. While data is clearly becoming one of the key assets on one side, ISs have to be highly integrated and open on the other side. Appropriate treatment of these issues is not a trivial task.

This chapter provides managers of intelligent enterprises with a new approach towards IS security management. It gives a necessary technical background and focuses afterwards on human resources, i.e., human factors management, which turned out during recent years to be the most important element to assure security of organizations' IS. The methodology is based on incorporation of business dynamics (Sterman, 2000) and business intelligence. Note that holistic management of IS security requires not only understanding of technological and organizational issues, but also appropriate coverage of system analysis and design, auditing issues, inter-organizational issues and legislation. For a complete and coherent treatment of these issues, a reader is advised to read (Trek, 2003).

## E-BUSINESS SYSTEMS SECURITY CONCEPTS

When protecting information, an organisation has to start with the identification of threats related to business assets. Based on threats, an approach has to be taken on two planes. The first plane covers interactions—it all starts with technology, where appropriate security services are realized by deployment of security mechanisms and consequently security services. To make things operational, key management that serves as a basis for human-machine interactions has to be resolved. Finally, human interactions have to be covered. In parallel, it is necessary to properly address the second (management) plane where human resources management is considered in relation to the technological basis.

## TECHNOLOGICAL BACKGROUND

### Threats Analysis, Security Mechanisms and Security Services

Every security related activity starts with threats analysis. Although threats analysis may vary from one specific environment to another, the basic approach is as follows (Raepple, 2001). Threats are