Foreword by
Dr. Bhuvan Unhelkar

WILEY

INFORMATION SYSTEMS SECURITY

Security Management, Metrics, Frameworks and Best Practices

NINA GODBOLE

Information Systems Security

Security Management, Metrics, Frameworks and Best Practices

Other Wiley Editorial Offices:

John Wiley & Sons, Inc. 111 River Street, Hoboken, NJ 07030, USA

Wiley-VCH Verlag GmbH, Pappellaee 3, D-69469 Weinheim, Germany

John Wiley & Sons Australia Ltd, 42 McDougall Street, Milton, Queensland 4064, Australia

John Wiley & Sons (Asia) Pte Ltd, 2 Clementi Loop #02-01, Jin Xing Distripark, Singapore 129809

John Wiley & Sons Canada Ltd, 22 Worcester Road, Etobicoke, Ontario, Canada, M9W 1L1

First Edition: 2009

ISBN: 978-81-265-1692-6

www.wileyindia.com

Printed at: *Unique Colour Carton, Delhi*

Contents

36 Privacy Best Practices in Organizations

Part I

Introduction

- **Chapter 1** Information Systems in Global Context
- **Chapter 2** Threats to Information Systems
- **Chapter 3** Security Considerations in Mobile and Wireless Computing
- **Chapter 4** Information Security Management in Organizations
- **Chapter 5** Building Blocks of Information Security
- **Chapter 6** Information Security Risk Analysis

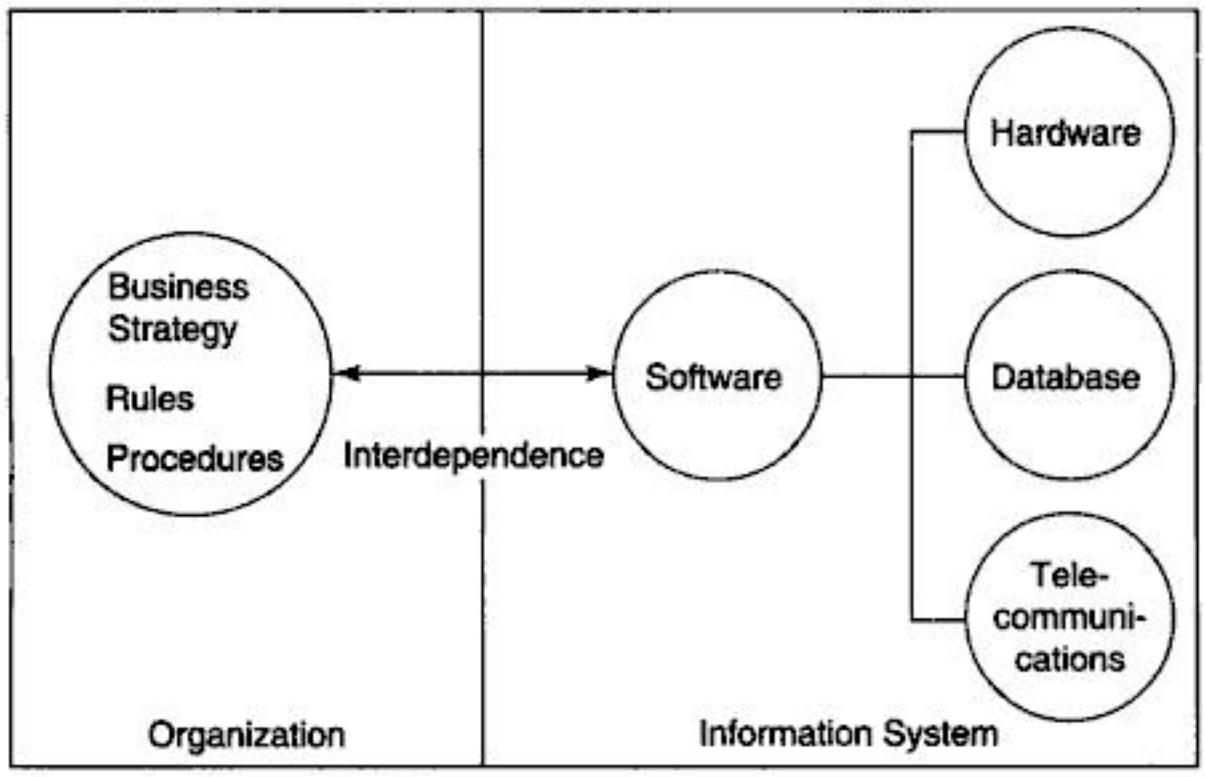

Figure 1.3 | Functions of an information system.

there are HR information systems and in marketing and sales area, there are CRM systems. It is important to note at this point that not all types of information can be computerized, especially the ones with an external source. Table 1.1 shows business area-wise organization of information.

Table 1.1 | Business area-wise information

Business area	Coverage	Typical examples	Remarks
Business environment	Business conditions external to the organization that can impact its business activities	1. Rules and compliance set by regulatory agencies 2. Issues created by competitors 3. Licensing authorities' requirements	These may not be handled in a computerized manner inside a company data warehouse
Customers and other affinity organizations	People and organizations who acquire and/or use the company's products	1. Prospects 2. Customers	Organizations use these mechanisms for capturing potential customers (prospects) and for distinguishing between parties who buy the product and those who use it
Communications	Messages and the media used to transmit them	1. Advertisement campaigns 2. Target audience 3. Company websites	These often pertain to marketing/ prospecting activities. They can also apply to internal and other communications
External organizations	Organizations, except customers and suppliers, external to the company	1. Complementors /business partners 2. Existing competitors 3. Potential competitors	In the paradigm of 'networked organizations' of today, this inclusion is important

Box 1.1 *Continued...*

customer service, while substantially reducing the amount of time and training required for common service operations. Client/server computing may also provide the best alternative for meeting new requirements for electronically interfacing with business partners; a service that is very crucial in electronic business (e-business) era.

An important point to note is that contrary to many predictions and common belief, client/server computing is not 100% replacing traditional mainframe-based application systems. Instead, a blended system seems to be emerging that combines the data-processing horsepower of the legacy mainframe applications with the opportunities for rapid application development and electronic interfacing capabilities of the client/server technology. The cornerstone of this solution is a three-tiered approach, in which an application layer provides an interface between the client/server system and the legacy mainframe system.

Box 1.2 Three-Tier Architectures for Information Systems

The three-tier architecture (also referred as the multi-tier architecture) was developed to overcome the limitations of the two-tier architecture. In the three-tier architecture, a middle tier was added between the user system interface client environment and the database management server environment. There are a variety of ways of implementing this middle tier, such as transaction processing (TP) monitors, message servers or application servers. The middle tier can perform queuing, application execution and database staging. For example, if the middle tier provides queuing, the client can deliver its request to the middle layer and disengage because the middle tier will access the data and return the answer to the client. In addition, the middle layer adds scheduling and prioritization for work in progress. The three-tier client/server architecture is known to improve the performance of groups with a large number of users (in thousands) and improves flexibility when compared to the two-tier approach. Flexibility in partitioning can be as simple as 'dragging and dropping' application code modules onto different computers in some three-tier architectures. A limitation with three-tier architectures is that their development environment is reportedly more difficult to use than the visually oriented development of the two-tier applications. Recently, mainframes have found a new use as servers in three-tier architectures.

The most basic type of three-tier architecture has a middle layer consisting TP monitor technology. The TP monitor technology is a type of message queuing, transaction scheduling and prioritization service where the client connects to the TP monitor (middle tier) instead of the database server. The transaction is accepted by the monitor, which queues it and then takes the responsibility for managing it to completion, thus freeing up the client. When the capability is provided by third-party middleware vendors, it is referred as 'TP Heavy' because it can service thousands of users. When it is embedded in the DBMS (and could be considered a two-tier architecture), it is referred as 'TP Lite' because experience has shown performance degradation when over 100 clients are connected. The TP monitor technology also provides:

1. the ability to update multiple DBMSs in a single transaction;
2. connectivity to a variety of data sources including flat files, non-relational DBMS and the mainframe;
3. the ability to attach priorities to transactions;
4. robust security.

Using the three-tier client/server architecture with TP monitor technology results in an environment that is considerably more scalable than a two-tier architecture with direct client to server connection. For systems with thousands of users, the TP monitor technology (not embedded in the DBMS) has been

Box 1.3 *Continued...*

3. *universal description, discovery and integration* (UDDI) and *the web services inspection language* (WSIL), used to find web services;
4. *WS-security*, used to manage *security across web services;*
5. *WS-coordination*, used to *coordinate multiple web services* into a larger composite system.

Many other web service standards remain under development. Organizations that publish these standards include the *World Wide Web Consortium* (W3C) and the *Organization for the Advancement of Structured Information Standards* (OASIS).

Benefits of web services for developing IS of global nature are as follows:

1. Web services tools are available for most computer systems, including mainframes and packaged applications. This means that not only the existing applications can be retained, but also the existing knowledge of staff can be applied and extended using web services for business integration.
2. Web services are adaptable and can handle changes more readily than other integration solutions, because they use structured text as their message format. Therefore, because the cost of maintenance is reduced, the overall cost of a web services system also reduces.
3. IT managers now have the ability to exchange data between most applications, on most computers, in a consistent and standard way. Tools and further standards are therefore emerging to build composite applications that can model and manage business processes around these business-level components.
4. If necessary, an alternative application can be used to provide web services without changing the overall effect of the system. This gives significant flexibility in the choice of a supplier. This aspect is particularly important in the consideration of outsourcing security services.

1.7 Information Systems Security and Threats: A Glimpse

So far, we have seen that the use of IS has become mandatory for businesses to perform their day-to-day functions efficiently. In this section, we set the context for understanding the issues related to IS misuse, resulting threats and countermeasures. This section is only an overview about threats to IS. It sets the stage for the detailed discussion taken up in the next chapter on the role of organization in security management.

Given the crucial role played by information systems, it is important that they remain secured and that the data contained in them do not fall into the hands of those who are not intended to have access to it. Security of IS becomes particularly important with the advent of the Internet. The access by Internet in particular allows a mass of information to remain up-to-date in real time, but it also opens the door for external encroachment. Thus, it is essential to ensure the physical protection of the information that, when stored without precautions on the hard disk of a computer connected to the Internet, can be read, copied, modified or destroyed from a working station located somewhere on the planet without the owner realizing the tampering.

In the modern business era, the use of desktop PCs, laptops, and network connectivity including the Internet and electronic mail (e-mail) is as essential as the telephone at workplace. The employees and networked IS are the most valuable assets for any organization. The misuse of information systems by employees, however, poses serious challenges to organizations including loss of productivity, loss of revenue, legal liabilities and other workplace issues. Organizations need effective countermeasures to enforce their appropriate usage policies and minimize their losses as well as increase the productivity of knowledge workers. The basics of *information systems security* are related to:

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.

You have either reached a page that is unavailable for viewing or reached your viewing limit for this book.