INTEGRATING SECURITY AND PRIVACY ISSUES IN SYSTEM DESIGN

Jan Guynes Clark[1], Nicole Beebe[1] and Andrew G. Kotulic[2]

[1]The University of Texas at San Antonio 6900 N. Loop 1604 West, San Antonio, TX 78258

[2]Kent State University P.O. Box 5190, Kent, OH 44242-0001

Abstract. Security and privacy issues are often an afterthought when it comes to system design. However, failure to address these issues during analysis and design could result in catastrophic effects. We propose a conceptual model for creating subsystems of security and privacy that are integral parts of the overall system architecture.

Keywords. Security, Privacy, System Design

1 Introduction

System analysts and designers strive to provide a system that meets the budgetary and business needs of an organization. While they may spend hours tracing the flow of data, few designers pay much attention to the potential security and privacy issues related to the system. We purport that these issues need to be addressed, starting at the earliest stages of analysis and design, progressing through the life of the system. Otherwise, the end result could be a costly, non-aligned system that fails to meet the business needs of the organization. Admittedly, the initial cost of the system would be greater, and the design time would be extended. However, the overall improvement in system efficiency, effectiveness, security, and privacy would be well worth the increased time and effort expended on the design. Additionally, the organization should consider the consequences of not considering security and privacy issues during system design. These could include exorbitant legal costs and civil penalties, along with reduced stakeholder trust.

We propose a conceptual model for system design based upon the integration and interaction of three primary subsystems: business processes, security, and privacy. For this paper, we will focus on the security and privacy subsystems. While no system can maintain maximum privacy and ensure security at all times, this should not prevent us from trying to attain these goals.

Security and privacy goals may seem conflicting and incompatible, especially if they are approached in the later stages of design, or after system implementation. However, if these issues are addressed in the early stages of design, both privacy and security can be attained at a reasonable level.

Guynes Clark J., Beebe N. and G. Kotulic A. (2004).
INTEGRATING SECURITY AND PRIVACY ISSUES IN SYSTEM DESIGN.
In *Proceedings of the 2nd International Workshop on Security in Information Systems*, pages 33-46
DOI: 10.5220/0002659400330046

2 The Systematic Approach

We followed Rechtin's [7] systematic approach to model building: 1) aggregate closely related functions, 2) partition the model into subsystems, and 3) integrate the subsystems into a functioning system. As you will see, there is considerable redundancy in our model. This was intentional. We contend that one's view of a component differs when considering how it relates to the business process, security, and/or privacy subsystem. For example, assume you are designing a patient billing system. While each of the subsystems is concerned with patient data, their view of the data is quite different. The business process subsystem utilizes patient data to charge a given patient for services provided; the security subsystem attempts to prevent patient information from being modified or accessed by unauthorized people; and the privacy subsystem attempts to limit the number of authorized people who can access the data.

We propose that one or more (depending upon project size) members of the design team be assigned responsibility for ensuring compliance with the security and privacy subsystems. Thorough analysis of these subsystems will provide a better understanding of the environment and aid in determining an acceptable level of risk. It will also provide justification for the need for additional expenditures in regard to security and privacy.

Since there is heavy interaction of the components of the system, there should be some degree of overlap among analysts and designers of the subsystems. Additionally, analysis of the components of each of the subsystems should be well documented and stored in a system knowledge database.

Although there is a close relationship between knowledge and data management, they are not the same. Knowledge is frequently fragmented, and signifies the relationships among information, or one's perception or understanding of a given concept. Both are concerned with acquisition and manipulation of data. However, knowledge management focuses on people, culture, and organizational structure, rather than technology.

Knowledge obtained during the system development process should not simply be stored in a database for archival purposes, never to be retrieved. Instead, it should be viewed, updated, and manipulated throughout the lifetime of the system, thus potentially enhancing the success of both current and future system development projects. Lessons learned should be included, because one frequently learns more from failure than success.

Our system framework centers around a shared knowledge base, accessible by everyone who has the need to know. Sharing of information and knowledge enables the analysts and designers to view their given subsystem in light of the other subsystems. This may aid in a better understanding of the system as a whole, and assist in alleviating or mitigating problems from the onset. Building the correct system is not enough. One must also build the system correctly.

2.1 Security Subsystem

The primary focus of the security subsystem (Figure 1) is protection of the organization’s information assets. These assets include information and data, software, hardware, people and procedures. In order to provide the appropriate balance between efficiency, effectiveness, security, and privacy of a system, the following components should be addressed:

2.1.1 Security Risk Analysis

The level of security applied to a system, or its components, should be commensurate with the level of assumed risk. Therefore, the system analyst and/or designer must be aware of the potential threats and vulnerabilities associated with the system. Many organizations, such as the Open Web Application Security Project (OWASP) [9] provide information on threats and vulnerabilities, along with steps to be taken to mitigate risks. However, these should be viewed only as guidelines. More pertinent information related to the given system should be obtained from the organization’s stakeholders. Once threats and vulnerabilities are determined, one must objectively evaluate the qualitative and/or quantitative impact of a given threat or vulnerabilities. Some threats may seem so remote that they simply are not worth considering, while others may seem imminent. For example, the designers should include password protection on a web-based system that provides access to customer accounts, but not necessarily on one that provides publicly available information. The steps in security risk analysis include the following:

- Identify the system functions, boundaries, and criticalities
- Identify security threats and vulnerabilities
- Evaluate qualitative and/or quantitative impact
- Calculate relative risk factors
- Design cost-effective controls for those threats and vulnerabilities with the greatest relative risk
- Document results of the security risk analysis in the system knowledge database

2.1.2 Data Evaluation

Systems exist in order to manipulate data. Data in some contexts may appear quite innocuous, yet when combined with other data, may be far more revealing. For example, most user ID’s are related to an individual’s name and can often be determined by simply viewing one’s email address. That by itself is not a major security threat. However, a perpetrator could also access the passwords associated with the user ID’s of pertinent personnel, potentially resulting in a major threat. Also, data may be considered secure within storage, but how secure is it when it is transmitted from one location to another? Security concerns of the following factors need to be considered:

- Determine the type of each data element within the proposed system – static, dynamic, or derived
- Determine how each data element is to be manipulated – create, store, access, process, transmit, print, and archive

- Classify the data according to access type -Public, Internal, Confidential, Restricted
- Document the data evaluation in the system knowledge database

2.1.3 Security Policies

Steps should be taken to protect data and information assets from unauthorized persons. Clearly defined policies and procedures help to emphasize management's commitment to maintaining security and privacy and instill a more secure culture within an organization. The need for these policies is greatly enhanced in organizations that interact with other entities by way of internetworks. Policy steps include the following:

- Review the security risk analysis to determine its impact on stakeholders
- Review and modify existing security policies, procedures, and documentation based on results of the security risk analysis
- Receive stakeholder approval, where appropriate, of new and/or updated policies, procedures, and documentation
- Distribute the revised policies to the appropriate personnel and stakeholders
- Assure that third parties are aware of the security policies pertaining to the proposed system
- Document security policy changes in the system knowledge database.

2.1.4 Security Legislation and Regulation

System designers must be aware of changes in the legal environment which may impact system requirements. This is always a daunting task, but compounded with organizations that conduct business across national borders. Some regulations, such as the United States' Health Information Portability and Accountability Act (HIPAA) apply only to one country, or group of countries. Others may be more pervasive, such as the Sarbanes-Oxley Act, which applies to all corporations (regardless of physical location) which are publicly traded on the U.S. financial markets [6]. We propose that a team approach be used to monitor the activities of the following bodies in order to deal with the many facets of this problem. The members should come from the security, audit, legal, management, IS/IT and HRM areas, as well as any other functional area, based on the impacted system.

- Review government agencies (Local and Foreign) for changes in security legislation
- Review industry regulatory groups for proposed changes in security practices and legislation
- Review international standards groups, such as the ISO, to assure compliance with the most current and proposed guidelines
- Revise security policies if deemed necessary
- Document changes in the system knowledge database

2.1.5 Security Architecture

As previously stated, security measures are not foolproof. Therefore, overlapping controls should be available to assure an adequate level of protection for the organization's information assets. The existing security architecture and supporting infrastructure should be reviewed and modified, as deemed necessary. A secure architecture requires assessment of every aspect of the system as well the network under which it operates. This includes:

- Review Business Continuity and Disaster Recovery plans
- Review Best Practices of the industry and organization
- Review business and system requirements
- Review physical and environmental protection procedures
- Review physical and system access controls
- Review computer system and application control
- Review information classification, access, and disposal controls
- Review network security infrastructure controls
- Document the changes to the security architecture in the system knowledge database

2.1.6 System Security Integration

System integration is the ability to seamlessly share data and resources across a variety of systems and platforms. Systems security integration takes this one step further by incorporating security into the process. The system designer must ensure that the proposed system security is not negatively impacted by other systems and/or platforms with which it may come in contact. Many organizations have formed strategic alliances which require fully integrated system communication throughout the supply chain. Therefore, the designer must consider the potential security consequences when systems are integrated. The following must be considered:

- Review integration of other systems and platforms within the organization
- Review integration with other systems and platforms external to the organization
- Review potential security risks
- Assess degree of access. Are you providing too much access?
- Assess potential legal and/or ethical ramifications of providing access across multiple platforms and/or organizations
- Establish a record of accountability
- Revise security policies as deemed necessary
- Revise security architecture as deemed necessary
- Document changes in the system knowledge database

2.1.7 Security Training

Policies and controls are of no value if the people expected to abide by them either do not know that they exist, or are not aware of their importance. Approximately 80% of all security breaches occur as a result of user actions (or inactions) that subsequently introduce vulnerabilities into the system [1]. Those who are aware of the consequences of a security breach are more likely to follow safe security practices. Therefore, it is imperative that all potential users be well informed of the importance of maintaining the security of the system, as well as potential consequences of failing to do so.

Security awareness training must be ongoing and should include all levels of the organization, including the top management team. Additionally, partners with whom information from the proposed system will be shared should be required to institute similar programs. The following factors should be considered.

- Provide security-based training to those individuals responsible for creating, storing, accessing, transmitting, printing, and/or archiving sensitive data
- Assure that all legal requirements have been met. For example, select industries such as healthcare and finance are required to provide select security awareness training
- Customize the training, incorporating appropriate policies and procedures
- Document security training (who, what, when, etc.) in the system knowledge database

2.1.8 Knowledge of Security Subsystem

As previously stated the knowledge gained from preparing the security subsystem is to be stored within the system knowledge database. This knowledge can potentially be referenced by system analysts working on the current system, as well as future systems. While some systems may remain relatively static for long periods of time, they are all, to some degree, dynamic. We therefore do not suggest that the knowledge database be your only source of information. Instead, it is to be considered a composite of knowledge regarding data, risk assessments, policies, legislation, training practices, and system architecture and integration over a given period of time.

2.2 Privacy Subsystem

The primary goal of privacy is to ensure the proper handling of personal information, such as one's finances or health status. Organizations can better build trust and customer loyalty if they can show the customers that their personal information is being protected. As with security, total privacy simply cannot be attained unless one lives in total isolation. The primary focus of the privacy subsystem (Figure 1) is to attain an acceptable level of stakeholder privacy. This should ensure that the organization in return merits the level of trust required to conduct its day to day operations with the stakeholder community. In order to provide the appropriate balance between efficiency, effectiveness, security, and privacy of a system, the following components should be addressed:

2.2.1 Privacy Risk Analysis

Potential risks to privacy of the individual and/or organization could arise with the introduction of a new system. Care should be taken in regard to the type of data related to the organization and its stakeholders, and how it is collected, stored, and disseminated. Designers must also consider how manipulation of this data might impact stakeholder perceptions of privacy protection. There appears to be a growing mistrust of consumers toward how organizations protect their personal information. Results in a recent survey showed that consumer confidence in how well businesses handled their personal information dropped from 65% in 1999 to 42% in 2003 [8] .

The steps in privacy risk analysis are the same as those in security risk analysis. However, the focus is on privacy, rather than risk. Those steps include the following:

- Identify privacy threats and vulnerabilities
- Evaluate qualitative and/or quantitative impact
- Calculate relative risk factors
- Design cost-effective controls for those threats and vulnerabilities with the greatest relative risk
- Document results of the privacy risk analysis in the system knowledge database

The analysts and designers should also make note of the following do’s and don’ts in an effort to improve the overall system, as well as improve stakeholder trust:

- Provide a means for stakeholders to determine what information is collected about them, and how it is used
- Provide a means for individuals to correct erroneous information about themselves
- Provide a means for individuals to opt in or out of the information collection, processing, or dissemination processes
- Obtain stakeholder consent before disseminating personal data with other organizations
- Do not share personal data with untrusted partners
- Assure the handling of personal data satisfies privacy legislation and abides by the organization’s privacy policies
- Review and/or update privacy policies
- Document results of the privacy risk analysis in the system knowledge database

2.2.2 Data Evaluation

Systems that maintain, use, or disseminate individually identifiable information should be designed in a manner to assure confidentiality, integrity, availability, and non-repudiation of the data. The old adage of “garbage in, garbage out” still applies. Data must be obtained from reliable sources, utilizing reliable data collection methods. Control mechanisms also need to be in place to protect against accidental or unauthorized data manipulation. Analysts and/or designers will evaluate the same data characteristics as described in the security subsystem, but their focus will be on data privacy, rather than data security:

- Determine the type of each data element within the proposed system – static, dynamic, or derived
- Determine how each data element is to be manipulated – create, store, access, process, transmit, print, and archive

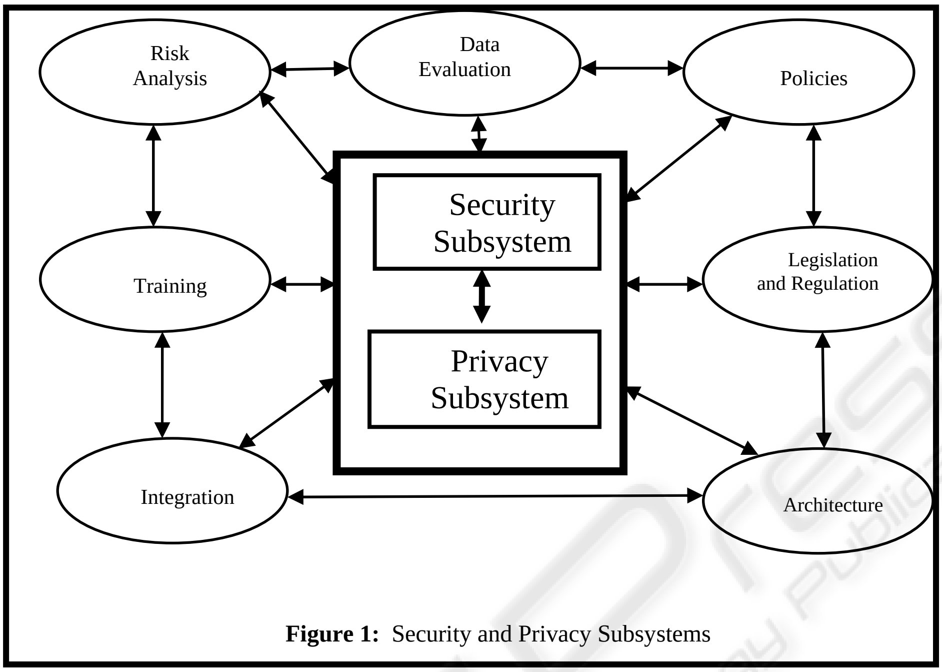

Figure 1: Security and Privacy Subsystems

- Classify the data according access type -Public, Internal, Confidential, Restricted
- Ensure proper protection and treatment of all personally identifiable data. Classify according to risk, value, ownership, and flow within the proposed system [4]
- Establish an audit trail
- Restrict information flow, when possible, when the risk of privacy loss is great
- Document the data evaluation in the system knowledge database

2.2.3 Privacy Policies

There is increasing privacy concern of internetworked systems. We have experienced an exponential rise in invasive software employed by third parties to collect user keystrokes and track their movement throughout the Internet [2]. While many marketers view this as a legitimate way of conducting business, most consumers consider this a violation of their privacy. Analysts and designers must be aware of these potential privacy invasions and take steps to mitigate them. Additionally, the designer must review the organization's privacy policies and design the system accordingly.

- Ensure the existence of a privacy policy that includes clear delineation and agreement with expectation of privacy "rights"

- Determine ownership and responsibility for the policy
- Review the privacy risk analysis to determine its impact on stakeholders
- Review and modify existing privacy policies, procedures, and documentation based on results of the privacy risk analysis
- Receive stakeholder approval, where appropriate, of new and/or updated policies, procedures, and documentation,
- Distribute the revised policies to the appropriate personnel and stakeholders
- Assure that third parties are aware of the privacy policies pertaining to the proposed system
- Document privacy policy changes in the system knowledge database.

2.2.4 Privacy Legislation and Regulation

As with security issues, system designers must be aware of changes in the legal environment that may impact how privacy issues should be considered when designing systems. Customers are becoming increasingly concerned about the data collected about them and how this data is disseminated. The EU is far advanced in preserving the privacy of the individual, while the United States is just beginning to address this issue. Regulations such as HIPAA and the Gramm-Leach-Bliley Act (protection of financial data) are helping to close the gap between the United States and the EU in this regard [5]. Again, we propose that a team approach be used to monitor the activities of the following bodies in order to deal with the many facets of this problem. The members should come from the security, privacy, audit, legal, management, IS/IT and HRM areas, as well as any other functional area, based on the impacted system.

- Review government agencies (Local and Foreign) for changes in privacy legislation
- Review industry regulatory groups for proposed changes in privacy practices and legislation
- Review international standards groups, such as the ISO, to assure compliance with the most current and proposed guidelines
- Ensure compliance with regulations by reviewing procedures for conducting privacy audits, reporting sensitive data, and handling breaches in privacy
- Determine the data to be protected – where is it? Who controls it? How is it accessed?
- Determine the consequences of breaches in privacy – how was it breached? How, and to whom, should the breach be reported? How can we prevent this occurring again?
- Revise privacy policies if deemed necessary
- Document changes in the system knowledge database

2.2.5 Privacy Architecture

The privacy architecture attempts to address privacy concerns as they arise and find ways to introduce privacy-enhancing components into the system architecture. At a recent Privacy Enhancing Technologies (PETs) workshop, the participants concluded that PETs should 1) provide the highest degree of anonymity possible, 2) minimize the amount of data collected about an individual, 3) focus on systems and infrastructures as well as tools, and 4) be designed within a system, rather than added at a later date [3]. Steps include the following:

- Determine privacy requirements
- Formulate potential solutions to the requirements
- Select the best solution, based upon needs of your organization and the data involved
- Integrate the solution with the system design criteria
- Document changes to the privacy architecture in the system knowledge database

The designer must ensure that the technologies being incorporated into the system do not violate the existing internal and external privacy policies. All too often, designers either assume that stakeholder privacy is not compromised, or simply are not aware of its importance. One should pay particular attention to such technologies and procedures as web server log files, cookies, known software bugs and patches, and sophisticated data mining algorithms.

2.2.6 System Privacy Integration

We define System Privacy Integration as the ability to seamlessly share data and resources across a variety of systems and platforms while concurrently protecting stakeholder and corporate privacy.

It is important that organizations routinely monitor and/or evaluate their privacy practices, as well as those of their business partners. The following must be considered:

- Review integration of other systems and platforms within the organization
- Review integration with other systems and platforms external to the organization
- Review potential privacy risks
- Revise privacy policies as deemed necessary
- Revise privacy architecture as deemed necessary
- Document changes in the system knowledge database

2.2.7 Privacy Training

Individuals must understand how to protect the privacy of data. They must also understand the consequences of what could happen when privacy has been breached. Individuals that interact with the proposed system must be aware of all pertinent privacy policies and be expected to abide by them. The need for privacy awareness training must be ongoing and should include all levels of the organization, as well as partners with whom the system information will be shared. The same factors considered for security should be considered for privacy.

- Provide privacy-based training to those individuals responsible for creating, storing, accessing, transmitting, printing, and/or archiving sensitive personal data
- Customize the privacy awareness training, incorporating appropriate regulations, policies, and procedures

- Document privacy training (who, what, when, etc.) in the system knowledge database

2.2.7 Knowledge of Privacy Subsystem

Please note that the system knowledge database may contain a lot of data pertaining to stakeholder privacy and organizational business practices. Therefore, it should be well protected from potential misuse. Only those with the need to know should be provided access to the knowledge database.

3 System Integration/Optimization

One must bear in mind that the privacy, security, and business process subsystems must be fully integrated (Fig. 2). This is a highly iterative process. A change in any of the components in any of the given subsystems requires review of all other components within the system in order to assure efficiency, security, and privacy of the system as a whole. This need for system integration further highlights the necessity of having an updated system knowledge database.

System design knowledge has traditionally been managed via system design documents and configuration management (CM) systems and processes. Such mechanisms, however, seldom document information protection objectives and matrix subsystem design components to those objectives. Traditional configuration management mechanisms primarily serve as inventory management aids, as well as organizational tools in software development environments.

Conversely, the systems knowledge database is intended to be a decision support tool. It helps analysts and developers who have different and sometimes contradictory information protection goals to make sound subsystem design decisions by considering the overarching information protection goals and the impact of changes on other subsystems.

A systems design knowledge database should store security and privacy objectives; results of the risk analysis, including asset identification and valuation, threats and vulnerabilities, and risk management decisions; and resultant subsystem design components implemented. Each design component should be mapped to a set of technical capabilities, as well as the overarching information protection goal(s) addressed by each component. This will facilitate better decision making in later design reviews. When new components are being proposed and legacy components are being considered for removal from the system design, the system knowledge database can be polled and assist in providing detailed information regarding the impact of such system design additions and deletions.

While optimizing the subsystems, the analysts and designers may note conflicts among the subsystems. Complying with one set of regulations or demands may result in the unintentional violation of others. Some conflicts can be addressed without negatively impacting system efficiency, security, and/or privacy, while others may not. As a result, trade-off decisions must be made, and one or more of the subsystems may have to be sub-optimized. Which is more important – security, privacy, or efficiency of the business process? There is no easy answer as to this question. We must be able to efficiently and securely collect, process, and store data while protecting the privacy rights of an identifiable entity. This dilemma is further compounded when one considers where this data is located, and where it may be disseminated. If it crosses national borders, the privacy and security concerns and regulations of each of the involved countries must be addressed.

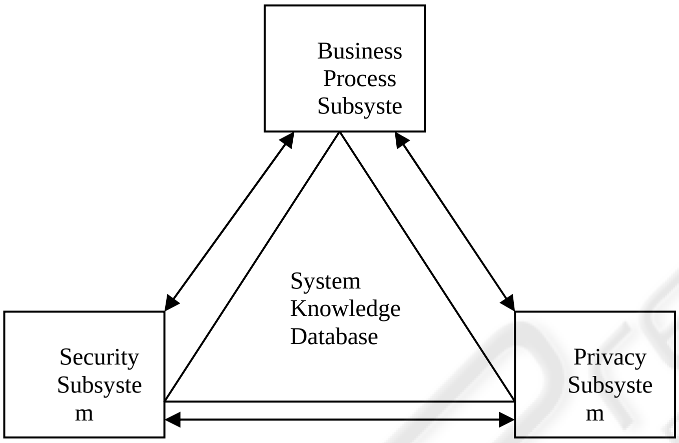

Figure 2: Fully Integrated System

Given a choice, most organizations would probably prefer to compromise the privacy subsystem. Why? Privacy generally impacts its stakeholders, rather than the organization itself; increased privacy controls can, and often do, impact system efficiency; and it is costly and time-consuming to protect stakeholder privacy. However, the organization runs the risk of losing stakeholder trust, which could have a very strong negative impact on the viability of the firm.

Although there is no easy answer to this question, we suggest the following:

- Consider the stakeholders and their level of involvement in the given system
- Identify stakeholder data which has security and/or privacy characteristics (i.e. patient medical records)
- Identify locations internal and external to the organization in which this data could be disseminated
- Perform security and privacy risk analyses
- Evaluate current regulations, policies, and best practices as they relate to the co-located data
- Categorize security, privacy, and business risks
- Address the risks in each category which can be mitigated in a costly manner
- Continually monitor the system throughout the life cycle for changes in security, privacy, and business process

4 Conclusions

As shown in Figure 1, while the components of the security and privacy subsystems are identical, the focus on these components is quite different. While we can never achieve maximum system efficiency within a totally secure and private environment, we can attempt to improve each of these subsystems by addressing them from the onset of system design.

This should lead to a functional system that has taken into consideration the following:

Concerns for security and privacy should not be considered a necessary evil; instead, they should be incorporated within the organizational culture, and viewed as arequirement for maintaining viability of the organization

- Although security and privacy breaches are inevitable, we must strive to reduce them and mitigate consequences of those that occur
- One’s employees remain the greatest security risk. Most security violations are unintententional, while others are the result of disgruntled employees. Therefore, organizations should assure their employees are well trained and satisfied with their jobs.
- Security is everyone’s responsibility – from the CEO to the first line employee
- The optimal level of security for an organization should be based upon the evaluation of the costs related to obtaining an acceptable risk level
- The major tradeoffs between cost, flexibility, and ease of use should be considered when designing the overall system.

Security and privacy are shared responsibilities. By integrating these susbystems with the business process during the early stages of system design, and by following the basic guidelines, the resulting system should be far more secure, effective, and trustworthy.

References

1. Cowens, B.: The Security Threat Inside: Building an Awareness Program and Effectively Training Your Staff. The ISSA Journal. November 2003. 10-12.
2. Lawton, G.: Invasive Software: Who’s Inside Your Computer? Computer. July 2002. 15-18.
3. Main Outcomes of the Technical Workshop on Privacy-Enhancing Technologies 4 July 2003. http://europa.eu.int/comm/internal_market/privacy/docs/lawreport/pet/200304-pet-outcome_en.pdf
4. Mathur, Sanjay.: Builing an Inside-Out Privacy Compliance Framework. The ISSA Journal. December 2003. 14-17.
5. Noor, A.: Dealing with data Privacy Regulations and SB-1386. The ISSA Journal. May 2003. 8-10.
6. Raval, V. Guidelines for Compliance with Sarbanes-Oxley. EDPACS . January 2004. 14-20.
7. Rechtin, E.: Systems Architecting: Creating and Building Complex Systems, Prentice Hall, New York 1991.

8. Taylor, Humphrey. Most People Are “Privacy Pragmatists” Who, While Concerned About Privacy, will Sometimes Trade it Off for Other Benefits. The Harris Poll # 17, March 19, 2003. Http://www.harrisinteractive.com/harris_poll/.
9. The Open Web Application Security Project (OWASP). January 13, 2003. The Ten Most Critical Web Application Security Vulnerabilities. http://www.owasp.org.