"1st International Symposium on Computing in Informatics and Mathematics (ISCIM 2011)"
in Collabaration between EPOKA University and "Aleksandër Moisiu" University of Durrës
on June 2-4 2011, Tirana-Durres, ALBANIA

Practical Guidelines and Major Issues in Information Security Management Systems Implementations

Lami KAYA[1,2]

[1]*Department of Computer Engineering, FATIH University, Istanbul-Turkey*
[2]*Department of Computer Engineering, YILDIRIM BEYAZIT University, Ankara-Turkey*
Email: LamiKaya@gmail.com – Phone: +90 533 387 13 88

ABSTRACT

Information is a major asset for any organization, to public or private. Threats to information and information handling resources are getting more sophisticated continuously. Also, regulatory requirements for data and system protection are increasing in number as well as complexity. There are number of frameworks to deal with these issues systematically and effectively. One of such framework is the ISO 27001 Information Security Management System (ISMS), which provides a framework for organizations to protect themselves against internal and external threats as well as natural disasters. The ISMS provides guidelines on how to manage information processing, storage and transmission with appropriate controls in order to avoid any security breaches. ISMS considers people, policies and IT technology as major categories of a security system. An organizations personal has to be trained for establishing, implementing, operating, monitoring, reviewing, maintaining and continuous improving ISMS. Implementation of ISMS requires role-model attitude from the top management. Without a visionary and supportive leadership, the ISMS cannot be used to properly identify and address the risks for an organization. The practices show that an effective ISMS operation may require major changes to some routine work practices. Clear direction from senior managers as well as coordination/support among team members is crucial for a successful ISMS project execution. In this work, some practical guidelines for successful, cost effective and functional ISMS implementation will be provided. Also, observations gathered from years of auditing trails and lessons obtained through practical applications will be presented. Major considerations for the success/failure of security systems shall be discussed. It is concluded that security is preparation of adequate policies/procedures/instructions and the support of well-informed/diligent people, rather than utilization of sophisticated high-technologies. The importance of human factor for the success such management systems will be exemplified with real-life cases.

INTRODUCTION

Information security (IS) has been a source of attention even in the medieval era. With the unprecedented developments in IT for information creation, processing, storage, sharing and transmission the need for IS is becoming more evident to everyone. As functionality improved and use of IT become easier, security concerns has increased and attacks on IT systems has grown almost exponentially. Also, the IS practice has become much more complicated and the need for qualified IS professionals has become critical. There have been many proposals and suggestions by academia, industry, governmental and non-profit national/international organizations to deal with these issues. Each of them having various degree of emphasis on different aspects of security. Majority of such schemes/methods remained as proprietary and a few successful ones moved to standardization stage. Some have been very popular and found wide acceptance among professionals, while some others stayed as theoretical suggestions. Generally speaking, proposals that came from consortium of academia, industry, governments and/or non-profit professional institutions covered the issue from different angles. Beside schemes that focusing on IS issues, there have been also methodologies on more generally IT management, governance and services. Each of IT related system had some parts dedicated to IS issues, some having wide IS coverage and some others looking through restricted/limited view of IS. Some have put lots of weight on technology, while others view issue mostly as a matter of management. There has also been call for more balanced view of technology and management in achieving effective and efficient IS.

SECURITY FUNDAMENTALS

Managing IS programs has become an increasingly difficult and challenging job as new technologies and popular applications (such as facebook) get wide acceptance among uniformed users. Remarkable advances in computing and communications technology is placing data processing focus on once so called "computing center" as well as individual connected/networked devices. The mobility and wireless technologies are making the security/privacy issues much more complicated. As these changes are accelerating, the IT security personal's job becoming increasingly difficult. The result is that security personal must now monitor security on a more widely dispersed level.

Security programs try to meet three fundamental requirements: the confidentiality, integrity, and availability of an organization's information resources. Some use CIA abbreviation to refer to these requirements. In some application, combination these requirements must be met, while in some other cases requirements may be reduced based on the nature of the application, operational environment, circumstances faced, etc. We'll look at CIA model components briefly in the following [1][2][3]:

Confidentiality is the protection of information so that unauthorized parties cannot access it. This type of protection can be thought as very important to only military/government organizations, however, in the business-oriented new world, businesses should protect their trade secrets from competitors or prevent unauthorized persons from accessing the company's sensitive information. Related concept of *privacy* also place immense importance on confidentiality for protecting personal information maintained on IT systems operated by governmental agencies or private-sector organizations. A crucial aspect of confidentiality is user identification and authentication. Confidentiality models are used to describe what actions must be taken to ensure the confidentiality of information [4][5][6]. These models can specify how to use security tools to achieve the desired level of confidentiality.

Integrity is the protection of information from intentional/accidental unauthorized changes. The challenge is to ensure that data is maintained in a state that users expect. Integrity is needed to protect information from unauthorized modification. A critical requirement for both commercial and non-commercial information processing is to ensure the integrity of data to prevent fraud and errors. An IS system can't do much on the accuracy of information that is put into the system by users, but it can help ensure that any changes are correctly applied and can be tracked. As with the confidentiality policy, identification and authentication of users are key elements of the information integrity.
Availability is the assurance that an information system is accessible by authorized users whenever needed. Major threats to availability are Denial of Service (DoS) and loss of information processing capabilities as a result of natural disasters or human actions. Considerable effort is being devoted to addressing various aspects of availability.

ISMS BASICS

The ISO/IEC 27001, part of the ISO/IEC 27000 family of standards, is an ISMS standard published in October 2005 (latest edition at the time of this writing) by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Its full name is ISO/IEC 27001:2005 - Information technology - Security techniques -- Information security management systems – *Requirements* [7][8]. There are number of supportive related standards. One of them is Information technology - Security techniques -- Information security management systems – *Code of practice for Information Security Management*, which is practical guide on implementation. The ISO/IEC 27001 information security management system (from this point onward to be referred to as ISMS) provides a set of policies to provide protection against risks on information assets of an organization. Generally speaking, organizations may have a number of IS controls. However, without a formal/standard ISMS framework, the controls tend to be somewhat disorganized or disjointed. There are also some other schemes such as COBIT [9] and ITIL [10], which also handle some security of the issues, however,

they are mainly focused on creating a governance framework for information and IT more generally.

Various types of risks exist on information and IT resources: such as, system failures, denial of service (DoS) attacks, misuse of resources (Internet/email/telephone), damage of corporate image/reputation, espionage, fraud, malware (viruses/worms/spyware), use of unlicensed software, etc. The main principle behind an ISMS is that an organization should design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets. By putting an effective ISMS in place ensures acceptable levels of IS risk. As with all management processes, the ISMS applies the typical "Plan-Do-Check-Act" (PDCA), or Deming cycle approach [7][8], as summarized in the Table 1.

Table 1 Summary of PDCA Cycle for ISMS Standard Implementation

Plan	Establish ISMS	Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving IS to deliver results in accordance with an organization's overall policies and objectives
Do	Implement and operate ISMS	Implement and operate ISMS policy, controls, processes and procedures
Check	Monitor and review ISMS	Asses, and where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review
Act	Maintain and improve ISMS	Take corrective actions, based on the results of the internal audit and management review or other relevant information, to achieve continual improvement of ISMS

The establishment, implementation, monitoring, review, maintenance and continuous improvement of an ISMS provide a strong indication that an institution/company is using a systematic approach for the identification, assessment and management of IS risks and address fundamental security requirements (CIA). Main objective of an ISMS is to implement the appropriate measurements in order to minimize or (possibly) eliminate the impact that various security related threats faced and vulnerabilities exist in an organization. Organizations such as banks and financial institutions, telecom operators, hospitals and health institutions and/or governmental (public) bodies need to address information security very seriously. Legal and regulatory enforcements (which aim

at protecting sensitive or personal data) as well as general security requirements makes these big organizations to allocate their resources and prioritize actions dealing with IS risks.

ISMS IMPLEMENTATION

The development of an ISMS framework requires number of actions. The main points are: definition of security policy, getting the support of administration, definition of ISMS scope, risk assessment, risk management, selection of appropriate/applicable controls and preparing statement of applicability (SOA), preparing all policies/procedures, internal auditing, and continuously updating/upgrading. The standard consists of standard requirements part (mandatory clauses 4 through 8, no exclusions possible, applicable to all types of organizations) and Annex part [7][8], which summarized in Table 2.

Table 2 ISO 27001 ISMS Annex Domains (2005 Edition)

A5 - Security Policy
A6 - Organising Information Security
A7 - Asset Management
A8 - Human Resources Security
A9 - Physical & Environmental Security
A10 - Communications & Operations Management
A11- Access Control
A12 - Information Systems Acquisition, Development and Maintenance
A13 - Information Security Incident Management
A14 - Business Continuity Management (BCM)
A15 – Compliance

The ISO 27001 ISMS annex consists of 11 security domains (A.5 through A.15) to provide layers of security, 39 control objectives (statement of desired results or purpose), and 133 controls (policies, procedures, practices, software controls and organizational structure) [7][8]. Depending on the type of organization, it's scope, size, complexity, field of activity, nature of business some of the control objectives or controls may be excluded. When such an exclusion is made, appropriate justifications for its exclusion should be provided.

ISMS IMPLEMENTATION GUIDELINES

Without a formal ISMS implementation, IS controls in organizations typically address only certain aspects of IT or data security, leaving non-IT information assets (intellectual property, patents, plans, etc) less well protected. Therefore, ISO/IEC 27001 requires that the management of an organization to perform the following [12][13]:

- Systematically examine the organization's IS risks, taking account of the threats, vulnerabilities and impacts
- Design and implement a coherent and comprehensive suite of IS controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks.
- Adopt an comprehensive management process to ensure that the IS controls meet the organization's IS needs on an ongoing basis.

There are many approaches that can be used in an ISMS implementation. However, the following list can give good idea of what to be done briefly:

- Setting business objectives
- Identifying information assets. Key information assets should be prioritized
- Securing organizational commitment. For an ISMS implementation to be successful, the project's objectives need to be understood and endorsed throughout the organization
- Developing an asset-based risk assessment and treatment plan. Prioritizing information assets and correlating against potential threats, an idea of the perceived risks can be developed
- Checking compliance requirements (legal/statutory/regulatory/contractual)
- Engaging all-parties involved (investors/managers/users/customers/partners). Entities involved in business processes need to be advised, monitored and controlled

The ISO/IEC 27001 certification [7][8][13], like other ISO management system certifications, usually involves a three-stage audit process:

- Stage 1 - is a preliminary, informal review of the ISMS. For example, checking the existence and completeness of key documentation such as the organization's IS policy, statement of applicability (SoA) and risk treatment plan (RTP).
- Stage 2 - is a more detailed and formal compliance audit, independently testing the ISMS against the requirements specified in ISO/IEC 27001. The auditors seek evidence to confirm that the management system has been properly designed and implemented.
- Stage 3 - involves follow-up reviews or audits to confirm that the organization remains in compliance with the standard. Certification maintenance requires periodic re-assessment audits to confirm that the ISMS continues to operate as specified and intended.

ISMS IMPLEMENTATION PITFALLS

As expected there are discrepancies between the theoretical work and practical realities. There are many issues needs to be considered during the implementation and afterwards. There are many reasons for unsuccessful or in effective ISMS implementations [11]. The main issue is the prospective of the those involved in ISMS implement. Since most of the implementers come from technical and IT background they tend to emphasis on technical aspects (hardware, software). How the reality is most of the security reaches are occurring because of people involved in the process. Actually, a balanced view of technology, people and management is required. We would like to present a list of some common pitfalls of ISMS implementation that are encountered during our interaction/visit to companies for either training, consultancy or auditing:

- Lack of senior management support or no clear direction from senior management
- Lack/unclear comprehensive ISMS project planning
- Considering ISMS as an IT project involving IT staff only, rather than viewing as the responsibility of the entire organization units/personal
- Lack of specific roles and responsibility regarding ISMS within the organization
- Scope misjudgment (unacceptable minimization/exclusions or unnecessary inclusions)
- Incomprehensive asset listing
- Incomplete or inadequate risk assessment process
- Improper interpretation of controls
- Difficulties in writing proper security policies, procedures & instructions
- Lack of proper documentation or records required by the standard
- Non-prioritization of tasks and milestones
- Lack of assurance for effectiveness of selected controls
- Inadequate internal audit activities/processes
- Difficulties in conducting regular management reviews and implementing suggestions
- Difficulties in developing comprehensive business continuity plans
- Lack of status checks. It is essential to develop key security metrics and measure them regularly to ensure ongoing improvement
- Lack of (effective) training
- Lack of awareness among all staff members
- Lack of rehearsals for effective application of policies/procedures/instructions
- Regarding ISMS as a time project activity, rather than considering it as a live process that requiring continuous refinements/improvements

CONCLUSIONS

In this work some of our practical experience gathered from practical cases. Some common practices for adequate and effective ISMS implementation are shared. Also, number of shortcomings that were observed during analyzing various implementations as cases studies are presented. It's pointed out that the essence of success/failure for an ISMS project mostly depend on the behavior of people involved, rather and buying/placing high-tech equipment. By highlighting various points along this line, we it is expected new implementers will be able use them and existing implementers can improve their systems.

REFERENCES

[10] Panko, Raymond (2010): "Corporate Computer and Network Security, 2/E", Prentice-Hall

[11] Stallings, William (2011): "Network Security Essentials: Applications and Standards, 4/E", Prentice-Hall

[12] Carr, H., Snyder, C and ,Bailey, B. (2010): "Management of Network Security", Prentice-Hall

[13] Landwehr, Carl (September 1981): "Formal Models for Computer Security", ACM Computing Surveys, 13 (3): 8, 11, pp. 247–278

[14] McLean, John (1994): "Security Models: Encyclopedia of Software Engineering", John-Wiley pp. 1136–1145

[15] Bell, David Elliott (Decemer 2005): "Looking Back at the Bell-LaPadula Model". Proc. of the 21st Annual Computer Security Applications Conf., Arizona, pp. 337–351

[16] British Standard Institute (BSI), (www.bsigroup.com)

[17] International Organization for Standardization, (www.iso.org)

[18] "COBIT: Framework for IT Governance and Control", (www.isaca.org)

[19] ITIL (IT Service Management) (www.best-management-practice.com)

[20] Swanson, M. et al (2003): "Security Metrics Guide for IT Systems", NIST

[21] Helmbrecht, U. (Editor) (2004) "IT Baseline Protection Manual: New", BSI

[22] "Information Security Management System", (en.wikipedia.org)