Information Security Management - A Practical Approach

Manik Dey, *Member, IEEE*

Abstract— **Information security is an important issue in today's business. Information security management can no more be done by merely a set of hardware and software. Rather, it requires a complete end-to-end system. Such a system is called Information Security Management System (ISMS). It requires special focus and participation from all levels of employees with full commitments and responsibilities in establishing such a system and implementing it within the organization. ISO security standards and government compliance regulations guide and enforce organizations about certain requirements and norms. Organizations need to build an ISMS by combining all the bits and pieces as per their business needs. This paper illustrates a practical approach, as a ready reference, to build an ISMS in a business organization.**

Index Terms—**Computer Security, Information Systems, Security, ISO 17799 / 27001 Standards.**

I. INTRODUCTION

In the present day world, every business depends heavily on information. In most cases, information has become the vital 'asset' called 'information asset' or 'intellectual asset' for the business. It is essential to protect this asset so as to ensure its *confidentiality*, *integrity* and *availability* (CIA) with the intention that the right information is available to the right people, at the right place and at the right time. Unsecured information cannot be guaranteed to be correct and available as expected. It can also be easily misused. Unsecured or misused information can lead to the loss of business and its reputation. It can even question the future existence of the organization.

Obviously so, managing security of information is as important as managing the core business. That is why business organizations are now more worried about the security of their information. Also, the legal and audit institutions expect every organization to follow certain security compliance regulations along with the implementation of an information security management infrastructure in its business. Therefore, building and implementing an appropriate information security infrastructure is a crying need for most business organizations.

Manuscript received February 27, 2007. M. Dey is with the Kuwait Institute for Scientific Research (KISR), Systems Development Department, P O Box 24885, Safat 13109, Kuwait. (Phone: 965-4989736; fax: 965-4989709; e-mail: mdey@kisr.edu.kw).

In this context, 'information' includes all forms of data, knowledge, documents, communications, conversations, messages, recordings, and images. Since 'information', 'information systems', and 'computers' are all interrelated, security of information mostly means protection of all related assets, including but not limited to, hardware, network, internet connectivity, software, application, database, data (both at rest and in transit), file, directory, hard copy reports, telephone, fax, documents etc., in such a way that only authorized and valid users are allowed to access them physically or otherwise.

This paper illustrates some of the major concerns and suggests steps to follow in establishing and managing a comprehensive end-to-end information security framework in an organization using already established standards. It involves technical and management issues such as risk assessment, classification of information, design of policies and procedures, implementation of protection mechanisms, roles, and responsibilities as well as human issues such as security culture, awareness, training, and motivation.

The subject gets its importance by the fact that in most organizations there is lack of analyzing the requirements systematically and taking effective measures to design a system which will safeguard the company's information on a long term basis. In most cases, security is not given priority at the time of designing and implementing the IT solutions. Many organizations do not have qualified security experts who can be responsible for establishing a secured IT environment. They do not have proper security policies and procedures enforced into the business.

This paper intends to help these organizations to become aware of the wider implications of information security in business and get a ready reference, to start with, for the solution to their existing security problems.

II. CORE CONCERNS – THREATS TO INFORMATION

Security of information has evolved with time and has gone through various stages of its nature and forms. Initially there used to be physical threats of theft and direct access attack on computers and these were handled with the help of locks, keys, guards, identity cards, and alarms. Next, there came the network and internet connection-based threats which were tackled well by using firewalls, Virtual Private Networks

(VPN), and Demilitarized Zones (DMZ) separating Intranet, Internet, Extranet and common zones. The recent and more dangerous threats are from viruses, infected messages, and fraudulent sites carrying spyware and committing various attacks such as phishing, pharming, domain high jacking, DNS cache poisoning etc. In fact, now we are fighting against all these multi-dimensional security threats simultaneously. Sophisticated hacking and cracking techniques have made very thin lines between internet, intranet, secured and non-secured zones. Hobby hackers, turned into cyber criminals, are attacking business sites in order to earn money fraudulently. Credit cards misuse and financial frauds such as TJX ID theft, Enron and WorldCom scandals are raising genuine doubts on the safety of e-commerce and reliability of the financial strengths of organizations. Wireless and mobile computing have added extra security concerns. Protection of business from external threats is not enough, major threats are coming even from the internal users.

Thus, information is continuously being threatened to be lost, stolen, accessed (physically or otherwise), blocked, misused or destroyed by people, viruses, malwares, natural disasters (e.g. earth quake, tsunami), man-made disasters (e.g. 9/11 attacks) and sudden failures (e.g. US black-out in 2003).

Time has come that we consider these threats seriously from business perspectives and take corrective measures with a view to minimize the risks. We have to face and combat the threats because the other option will be to avoid using the information systems or technology and probably go back to the ancient age!

III. INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Organizations sometimes spend substantially on firewall, proxy, antivirus, intrusion detection mechanism, digital signatures, special network devices and protocols etc., assuming that security of information can somehow be ensured by procuring these technology solutions from the market. This is a wrong notion because security management is more of managing an end-to-end system rather than just installing technical solutions. As like any other full-fledged system, this has many components including people, policies, procedures, processes, standards and technology.

Development of an information security system is not that easy. Such a system should be purely value-based and business driven. There should be proper analysis and design, involving all the components mentioned above. Employees, starting from the senior management to the end users, should take appropriate role in establishing and implementing information security system within the organization. Processes need to be defined with specific business objectives to protect the 'information assets'. Technology solutions need to be implemented appropriately to fight against the threats and risks or to automate certain processes. Policies and procedures need to be established in order to define who will do what, when and how in order to prevent the threat, detect once it has occurred, and take corrective measure to fix the damages, if any. There should be a cultural change too within the organization to deal with information and its security in general. For example, an employee should not hand over his/her password to the other colleagues on a friendly basis while he/she proceeds on vacation. Instead, he/she should transfer the privileges to the designated persons through proper channel and revert back the status at the end of the vacation. People have to be mentally prepared or somehow be motivated to accept the importance of security and follow the rules.

All the above components are required to be linked into a system which should be implemented carefully to tackle the existing and newer security threats. Such a system is called *Information Security Management System (ISMS)*, the outcome of one of the most strategic corporate decisions and foundation of information security in an organization.

From the prospective of business, it is obvious that there should be additional investment on various resources while establishing an ISMS. Question comes, how much to invest? The investment will depend on the vulnerabilities, the risk factors associated with the business and its type, kind and size. Obviously, such investment should not outweigh the worth of information and assets being protected. The recent surveys conducted by CSI/FBI, indicate that majority of organizations spend 10-13% of their total IT budget on security of information [1]. The benefit of having an appropriate ISMS will always justify such investment.

IV. INFORMATION SECURITY STANDARDS

We have already established the essence of implementing an ISMS in an organization for the protection of its information. But how can we guarantee the success of this system? How can it be assured to be fully comprehensive in tackling all aspects of information security in the current situation as well as in the future developments? Here arises the need for standards and guidelines. Fortunately for us, there are international standards already available. These standards provide systematic management approach to adopt the best practice controls, quantify the level of acceptable risk and implement the appropriate measures which protect the confidentiality, integrity and availability (CIA) of information.

BS 7799 standard was established by British Standard Institute (BSI) in 1995 [9]. ISO 17799 has been derived from BS7799 in 2000. ISO 17799 Part 2 (2002) established the code-of-practice and the specifications of an *Information Security Management System* (ISMS) [9]. ISO/IEC 27001 (Nov. 2005) has been prepared to reemphasize the code-of-practice of ISO 17799 with few amendments and additions of controls that will enhance and improve the ISMS further [10].

ISO 17799 consists of a full cycle, from the consolidation to implementation, of an ISMS with code-of-

practice. It includes taking decision to adopt ISO 17799 as standard, assignment of resources, determining scope, reviewing documentation, analyzing gap, establishing information asset inventory, assessment and management of risks, establishing controls and objectives, developing policies and procedures, conducting awareness training, adopting and monitoring compliances.

ISO/IEC 27001 standard provides a robust model for implementing the principles in earlier guidelines. It governs risk assessment, security design, implementation, security management and reassessment. It adopts Plan-Do-Check-Act (PDCA) model reflecting the principles as set out by the Organization for Economic Co-operation and Development (OECD) in 2002[11]. The whole cycle consists of Plan (to establish an ISMS), Do (to implement and operate the ISMS), Check (to monitor and review the ISMS) and Act (to maintain and improve the ISMS) as shown in Fig 1. It also insists on 'Third Party Audit' and acquiring ISO 27001 certification in the same way as ISO 9000 series quality certification.

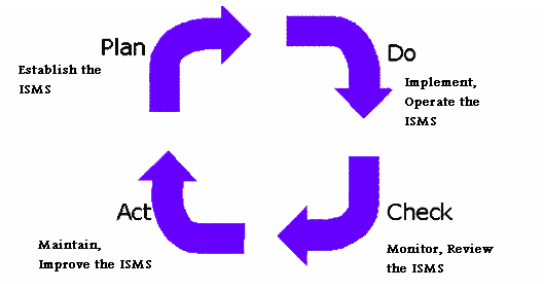

Fig 1 - PDCA Model

Further revisions of these standards as well as introduction of more new standards are on the way. For example, ISO BS25999 has been published very recently to define standards for Business Continuity in compliance with ISO 17799 and ISO 27001 [14].

Organizations, looking for information security solutions, should follow the ISO guidelines, design an ISMS as per their requirements, take management approval and implement the same with continuous tuning to make it effective in meeting the dynamic security challenges and compliance regulations.

V. INFORMATION SECURITY COMPLIANCES AND REGULATIONS

All is said and done. Still it is not enough. In presence of all the standards, policies, procedures, auditing etc, there had been lapses, data and identity thefts, money laundering, frauds, scandals through malpractices or misuse of information and disasters. Some organizations affected by such lapses and disasters had to face serious consequences including even shutdown. With the perception that these companies did not take sufficient measures to protect against these threats and in order to minimize the occurrences of such disasters, governments and competent authorities enforce organizations to follow certain compliance regulations as legislative mandates according to the type and kind of their businesses. These compliances and regulations are put in place to complement the ISO security standards.

In the recent past, these compliances have positioned themselves to be the vital requirements to ensure information security. For example, the Sarbanes-Oxley Act (SOX) is one of the most important legislations regulating corporate governance and financial disclosure for local and global organizations doing business in the US. A key issue in implementing the SOX is in measuring and planning acceptable levels of compliance for the IT systems. The CEOs, CFOs and CIOs (C-Levels) take responsibility and sign off the financial statements certifying that the levels of controls over the financial reporting processes and the security, accuracy and reliability of the associated information systems are adequate and as per business norms.

The rapidly growing use of information technology in various businesses and the transition of sensitive information into digital records have led to the formation of many such compliances, guidelines, regulations and regulating bodies. Here is a list of some of them.

- Sarbanes-Oxley Act (SOX) – compulsorily applies to all public companies
- Health Insurance Portability and Accountability Act (HIPAA) – applies to any organization handling health information about an individual
- Gramm-Leach-Bliley Act (GLBA) – applies to any financial institution and the companies that provide services to the institution
- California Security Breach Notice Act (formerly SB 1386) – requires companies maintaining data on California residents to inform individuals of any security breaches associated with their personal information
- European Safe Harbor Registration (European Data Protection) – data safety norms for all international firms with offices both in the US and in the EU
- Homeland Security Presidential Directives (HSPD-12) – directives for a common identification standard for US Federal employees and contractors
- Federal Financial Institution Examination Council (FFIEC) – guidelines for enhanced multilayer authentication procedure for banking institution
- The Committee of Sponsoring Organization of the Tradeway Commission (COSO) – common definition of internal control, standards and criteria against which organizations can assess their control systems
- Payment Card Industry (PCI), Data Security Standards (DSS) - govern the security standards for the most payment industries (Visa, MasterCard, etc.)
- Freedom of Information Acts 2000 - UK government legislation defining what information public sector organizations are obliged to provide on request

- Federal Information Security management Act (FISMA) – US Federal law as e-government Act, imposes a mandatory set of processes to be followed
- Control Objectives for Information and Related Technology (COBIT) – best practices for better control, audit and measurement
- The Information Technology Infrastructure Library (ITIL) – best practices for better IT services
- Information Security Forum's (ISF) Standard of Good Practice – guide to manage the business risks associated with organization's information systems
- Statement of Auditing Standards (SAS) 70 - defines the audit standards in order to assess the contracted internal controls of a service organization

In addition to demonstrating alignment with security policies and procedures in line with ISO 17799/27001 standards, organizations need to establish the above compliances, regulations and audit standards according to their nature of businesses. Violation of these regulations may be subject to unacceptable audits, penalties, liabilities, punishments to C-Level executives, and even complete closure of business.

VI. BUILDING AN ISMS FRAMEWORK

Adopting the principles of ISO 17799, ISO/IEC 27001 [9, 10] standards and norms of compliance regulations, an ISMS framework can be designed as follows:

1) *Information Security Policy:* Develop an information security policy document with clear scope and boundaries taking into consideration of the type of business, its location, assets and technology with proper justification of any area being excluded from the scope and boundaries. This policy document is an overview of security needs and a top tier of the security scheme. It defines assets to be protected and the extent of their protection. It is a formally approved corporate management policy document and a proof that the management has taken appropriate measures in establishing information security for the protection of organization's information against all possible threats.

2) *Organization of Information Security:* Define information security team with allocated responsibilities and commitments. Set up authorization process, confidentiality, non-disclosure terms and proper communication procedures within this security structure. Establish security terms for external parties (vendors, partners, contractors and suppliers).

3) *Asset Management:* Identify information assets with responsible owners. Define rules for the acceptable use of these assets from security point of view. Classify assets using any standard classification mechanism such as 'Sensitive', 'Confidential', 'Private', and 'Public' along with handling, labeling and disposing procedures.

4*) Human Resources Security:* Establish security check procedure in recruitment process (employees, part-timers, contractors) including non-disclosure terms in the employment agreement. Define security roles and responsibilities within the job description. Include security terms in transfer, leave, termination, resignation, retirement, etc. with appropriate clauses of disciplinary measures in case of violation.

5) Physical and Environmental Security: Ensure physical security in information and computer facility areas including computer center, delivery area, collection area, disposal/removal points. Ensure protection and maintenance of boundary, environment, fire protection, air conditioning, cables, power supply, locks and alarms. Establish log registry system for users, visitors and equipments coming in or going out of information facility areas.

6) Communication and Operation Management: In order to ensure security and correctness of information processing, write down procedures and responsibilities for all related operations including housekeeping, change/update management, segregation of duties, software or service acceptance and deployment criteria (in-house, outsourced), network protection (wired, wireless, mobile), e-commerce , clock synchronization, backup, recovery, exchange or transfer of data media, exchange of communication, use of e-mail, fax and handling of public information. State monitoring mechanisms including maintenance of audits and logs.

7) Access Control: Define procedures and responsibilities for all access related tasks. This will include user creation/registration for network (wired, wireless, mobile, and dialup), operating system, application and databases, allocation of rights and privileges, use of system utilities, port open/close criteria, monitoring of password, and access to critical systems, etc. Monitor access to information by maintaining audits and logs.

8) Information System Acquisition, Development and Maintenance (in-house or outsourced): Specify formal requirements of security controls in new system development, upgrade or modification of any existing system, testing, implementation, processing, input/output, message validation, and operating system changes. Specify procedures to protect application sources and objects. Identify procedures for using encryption, digital signatures, certificates and public key infrastructure (PKI) wherever necessary. Ensure that any third party software is malware free.

9) Information Security Incident Management: Define responsibilities and procedures to handle every possible security incident and weakness. Establish contingency plans for quick recovery of systems or services in case of failures. Specify mechanism of communication, reporting, collection of evidence, logs, audits, analysis, documentation of incident and solution.

10) Business Continuity Management (BCM): Define business continuity processes by identifying and prioritizing critical business areas. Perform threat and impact analysis for events which can cause interruption to business. Develop consistent business continuity framework in terms of time gap between failure and continuity. Design comprehensive data retention and backup policy along with recovery procedures. Arrange for preventive maintenance for all critical hardware, network, software, databases and applications. Develop replication or online backup site for mission critical e-

commerce system. Train employees on the business continuity plans along with live tests. Update continuity plans effectively in accordance with any change in business or policy.

11) Security Compliance: Comply with all legal requirements applicable to your business as per local or international regulations by identifying the needs and defining implementation procedures with allocated responsibilities. Comply with respective intellectual property rights and software copyrights. Safeguard organization's records and privacy of personal information. Perform security compliance reviews in policy matters as well as technology areas to ensure that appropriate procedures are followed in order to achieve the acceptable level of compliances. Perform system audits in compliance with the statutory regulations by the government and other authorities.

The above is a sample guideline taking into consideration of the most regular information assets. It may require to be changed according to different business situations by adding, deleting or amending subjects of attention in different areas.

VII. ISMS IMPLEMENTATION STEPS

The following is a list of steps which can be followed while implementing an *Information Security Management System* (ISMS) in an organization along with the ISMS framework established earlier.

1) Form an information security technical team, section, department or division with head designated as say, Chief Security Officer (CSO), if not done before.

2) Define an executive committee for the Information Security project approved by and comprising of people from Board of Directors, CEO, CIO, senior managers and managers.

3) Define a security implementation team comprising of selected people from the technical team, executive committee and relevant business areas within the organization.

4) Educate the implementation team with the latest standards, compliances and best practices for such kind of information security management project. Follow the standards in every step so that you do not skip any areas of importance. Take help from qualified consultants, if required.

5) Accomplish a comprehensive analysis of risks and vulnerabilities associated with various 'information assets' with respect to their security classification established earlier and their roles in the business.

6) For every asset to be protected, identify the extra security measurement needed with respect to the existing ones and the possible resources required for the purpose. Establish a matrix chart as an outcome of this exercise.

7) Prepare the project proposal with implementation plan along with the resource requirements (current and ongoing) including hardware, software, training, manpower and commitments. Present the project proposal to the executive committee for approval. Include the recommended changes, if any and arrive at the final approved proposal.

8) Write down 'Policies', and 'Procedures' documents covering all pertinent areas as analyzed before and using the security framework established in *Section VI*.

As indicated earlier, a security "Policy" typically outlines high level requirements of security controls or rules that must be met for a particular area or asset. A security "Procedure" is typically a collection of very clearly written system specific step-by-step guidelines which are strongly recommended to follow in order to implement the related policy effectively.

For example, a "*Backup and off-site media storage*" policy may mention that company's critical databases should be backed up everyday at 1:00 a.m. and the tapes media should be transferred to off-site safe by 10:00am. The procedure for the above policy would mention the details of all the critical databases including the type of backup (cold backup, hot backup), the backup cycles (full, incremental), the transfer and rotation policy (retention period) of media, labeling of the tapes, keeping safe lock and key, maintaining log or registry, etc. Each policy and procedure is addressed to appropriate audience (users, managers, IT staff, partners, vendors). In general, any policy or procedure will have paragraphs such as Scope, Objectives, Audience, Responsibilities, Requirements, Enforcement clause, Revision Date, Definition of Terms and Other References wherever applicable [6]. Sometimes, the policies and procedures are written in a single document. In that case, the above policy and its procedure can be a single section of the whole document with the section name as "*Backup and off-site media storage*".

Once all the policies and procedures are covered, it is suggested to prepare a summary *coverage matrix* showing the policy and sub-policy issues row-wise and with column-headings as Analysis-output, Policy no, Policy statement, Procedure reference number, Audience, Responsibility, Status and Comments. TABLE I shows one sample part of this summary matrix. This matrix will help in referring different policies and procedures with proper numbers and also help controlling the status of implementation.

9) Present the policies and procedures documents (or the single combined document) to the executive committee for refinement and final management approval.

10) Implement the project in phases according to priorities. The phases must have been defined earlier in the implementation plan. Any procurement of hardware, software, etc. should be linked with the implementation phases.

11) Along with other compliances, adopt some of the best practices such as ITIL, COBIT and ISF's standards as referenced in the list of compliances (*Section V*).

12) Organize awareness training for the employees to make them understand the security policies and procedures to be implied upon them. Ensure that the policies and procedures are circulated to all divisions and departments within the organizations and to outside parties, if applicable.

13) Establish procedures for periodic security vulnerability and penetration tests at sensitive areas. Review, evaluate and

refine the ISMS following the PDCA cycle.

TABLE I
SECURITY COVERAGE MATRIX

Policy Issue	Analysis -output	Policy no	Policy Statement		Com-ment
…					
4.Human Resource Security	….			.	…
4.1Prior to employment	…..	…..	…..	.	…
4.2 During employment					…
4.3 Change, Termination, Retirement	…..	….	……		…
4.4 Vacation/ handover	…..	…..	…….		…
…..					

14) Audit the information security framework and its operation by a competent auditor recognized by authority such as *Information Systems Audit and Control Association (ISACA)*. Make plan to acquire information security certification.

Certainly, the implementation steps will vary from business to business depending on the present status of the security infrastructure. The above steps have been formulated with the assumption that the project will start from scratch and end with successful implementation of an ISMS framework followed by achieving the ISO security certification.

VIII. CONCLUSION

Information security management is a continuous process. The ISMS along with policies, procedures and compliances should be reviewed and updated to match with the latest market trends and requirements. The cycle of review, gap analysis and update will ensure the long term benefits to the organization by protecting its IT assets in the most effective manner.

Understanding the importance of security implementation is very crucial. If employees do not understand the necessity of it, they may not take part in the implementation wholeheartedly and it may lead to failure of the project or delay in achieving results. The senior management, being the prime sponsor and motivator of the project, plays an important role in this matter from the very beginning.

The security solution should be carefully designed to achieve cost-effectiveness and return-of-investment (ROI) adding business values, apart from satisfying the compliance regulations keeping in mind that the investment on information security is an insurance cost which will protect organization's information from loss or destruction, avoiding downtime and thus increasing productivity.

The success of an *Information Security Management System (ISMS)* lies in the best combination of *People*, *Policies*, *Procedures*, *Compliances, Standards*, *Processes*, *Products* and *Technology*.

REFERENCES

[1] Lawrence A Gordon, Martin P. Loeb, William Lucyshyn, Robert Richardson, *2006 CSI/FBI Computer Crime and Security Survey (GoCSI.com)*.
[2] Virus Radar Website, [Online]. Available: http://www.virus-radar.com
[3] Maria Cirino, *Preempting Data Warfare: The Art of Comprehensive Vulnerability Management*. (www.blackbooksecurity.com).
[4] Amanda Andress, *Surviving Security,* 2004.
[5] Anonymous, *Maximum Security by Macmillan Computer Publishing USA* , 2001.
[6] Charles Cresson Wood, *Information Security Policies Made Easy,*2002.
[7] Alexander, Michael, *The Underground Guide to Computer Security, Addison-Wesly Publishing Compan,*1996.
[8] Gartner website. [online]. Available: http://www.gartner.com
[9] British Standards Institute, *Information security management, part 2*: "Specification for Information Security Management Systems. Technical Report BS 7799-2", 1999.
[10] ISO. ISO/IEC 17799:2000 –Information Technology –Code of Practice for Information Security Management. Technical Report. International Organization for Standards, Geneva, Switzerland, 2000.
[11] ISO. International Standards ISO/IEC 27001, "Information technology Security techniques - Information security management systems – Requirements", 2005.
[12] Lexis Nexis,Mathew Bender, "The Sarbanes-Oxley Act of 2002: with analysis", Newark, NJ, United States, 2002.
[13] Organization for Economic Co-operation and Development,"The Revised OECD Principles of Corporate Governance". Paris, 2004.
[14] "BS 25999:2006 Code of Practice for Business Continuity Management (BCM)". [online]. Available http:// www.bsi-global.com/
[15] "Information Security Survey. Technical report", Ernst & Young LLP, Cleveland OH, USA, 2004.
[16] Jan Eloff , Mariki Eloff, "Information Security Management – A New Paradigm", Proceedings of SAICSIST 2003 , Pages 130-136.
[17] United States General Accounting Office (GAO). "Executive Guide , Information Security Management – Learning from Leading Organizations", May 1998.
[18] Micki Krause, Harold F. Tipton, *Information Security Management Handbook.*
[19] Simson Garfinkel and Gene Spafford, *Practical Unix and Internet Security*, 2nd Edition.
[20] William Cheswick and Steven Bellovin, *Firewalls and Internet Security*.
[21] Deborah Russell and G.T. Gangemi Sr, *Computer Security*.
[22] Larry Hughes, *Actually Useful Internet Security Techniques*.