Research Paper Computer Science

Isms Framework in Design and Analysis of Information Security

Sharanappa Patil | Assistant Professor, Department of Computer Science, L.V.D College, Raichur-584103, Karnataka, India.

ABSTRACT

An information security management system (ISMS) is a set of policies and procedures for systematically managing an organization's sensitive data. The goal of ISMS is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach. This paper gives the details of about the ISMS and its significance in business where information security plays a vital role. The ISMS gives the information security measures for the business to deal with the issues relating to the security breach.

An ISMS typically addresses employee behavior and processes as well as data and technology. It can be targeted towards a particular type of data, such as customer data, or it can be implemented in a comprehensive way that becomes part of the company's culture.

KEYWORDS Security, Information Security, Security Breach.

INTRODUCTION

An information security management system[1] (ISMS) is a set of policies concerned with information security management or IT related risks. The idioms arose primarily out of BS 7799.

The governing 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, thus ensuring acceptable levels of information security risk.

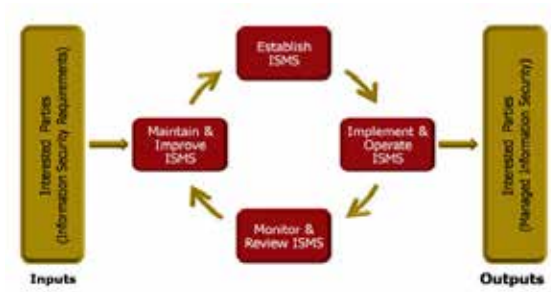


Fig 1: ISMS Architecture [1]

Best way to choosing an office security system

We talk frequently about cybersecurity, discussing how to protect your business's data by using strong passwords, deploying antimalware utilities, and keeping your computers safe with the latest patches and updates. This time, the focus is on premises security, or protecting your business's physical assets from burglary and vandalism.

The best cyber security measures in the world are useless if a thief breaks into your office and makes off with your computers.

You won't lose any digital data if you've followed our advice to back up your computers to secure, offsite locations; but if your business is like most operations, it isn't entirely digital. You have paper records, including sensitive personal information about your employees.

Your business also depends on physical assets—computers, displays, servers, fax machines, and everything that goes with them—that you will need to replace if someone steals them or destroys them. Can you afford that kind of disruption?

The latest security systems can not only alert you to a break-in, trigger an alarm, and dispatch law enforcement, but can also provide video surveillance, manage the HVAC (heating, ventilation and air conditioning) system, control the lighting, automatically power down small-office equipment according to a schedule, and in some cases provide access control.

Think you can't afford a security system? You'll be surprised at how inexpensive these systems can be. I'll discuss three examples: a do-it-yourself system from FrontPoint Security, a custom-installed system from ADT, and an access-control system from RedCloud that's designed for a larger company's IT department to manage.

The Success Factors For Information Security Management System

To be effective, the ISMS must

- Have the continuous, unshakeable and visible support and commitment of the organization's top management;
- Be managed centrally, based on a common strategy and policy across the entire organization;
- Be an integral part of the overall management of the organization related to and reflecting the organization's approach to risk management, the control objectives and controls and the degree of assurance required;
- Have security objectives and activities be based on business objectives and requirements and led by business management;
- Undertake only necessary tasks and avoiding over-control and waste of valuable resources;
- Fully comply with the organization philosophy and mindset by providing a system that instead of preventing people from doing what they are employed to do, it will enable them to do it in control and demonstrate their fulfilled accountabilities;
- Be based on continuous training and awareness of staff and avoid the use of disciplinary measures and "police" or "military" practices;
- Be a never ending process[3].

Asset (computer security)

In information security, computer security and network security an Asset is any data, device, or other component of the environment that supports information-related activities. Assets generally include hardware (e.g. servers and switches), software (e.g. mission critical applications and support systems)

and confidential information. Assets should be protected from illicit access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the organization.[2]

Information security
Information security, sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc.)[3]

Basic principles of information security Key concepts
The CIA triad (confidentiality, integrity and availability) is one of the core principles of information security (The members of the classic InfoSec triad -confidentiality, integrity and availability - are interchangeably referred to in the literature as security attributes, properties, security goals, fundamental aspects, information criteria, critical information characteristics and basic building blocks.) There is continuous debate about extending this classic trio. Other principles such as Accountability have sometimes been proposed for addition – it has been pointed out that issues such as Non-Repudiation do not fit well within the three core concepts, and as regulation of computer systems has increased (particularly amongst the Western nations) Legality is becoming a key consideration for practical security installations.

In 1992 and revised in 2002 the OECD's Guidelines for the Security of Information Systems and Networks proposed the nine generally accepted principles: Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Management, and Reassessment. Building upon those, in 2004 the NIST's Engineering Principles for Information Technology Security proposed 33 principles. From each of these derived guidelines and practices.

In 2002, Donn Parker proposed an alternative model for the classic CIA triad that he called the six atomic elements of information. The elements are confidentiality, possession, integrity, authenticity, availability, and utility. The merits of the Parkerian hexad are a subject of debate amongst security professionals.

In 2013, based on the extensive literature analysis, the Information Assurance & Security (IAS) Octave has been developed and proposed as an extension of the CIA-traid. The IAS Octave is one of four dimensions of a Reference Model of Information Assurance & Security (RMIAS). The IAS Octave includes confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability and auditability.' The IAS Octave as a set of currently relevant security goals has been evaluated via a series of interviews with InfoSec and IA professionals and academics. In,definitions for every member of the IAS Octave are outlined along with the applicability of every security goal (key factor) to six components of an Information System.

Integrity
In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of consistency as understood in the classic ACID model of transaction processing. Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

Availability
For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system essentially forcing it to shut down.

Authenticity
In computing, e-Business, and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be. Some information security systems incorporate authentication features such as "digital signatures", which give evidence that the message data is genuine and was sent by someone possessing the proper signing key.

Non-repudiation
In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

It is important to note that while technology such as cryptographic systems can assist in non-repudiation efforts, the concept is at its core a legal concept transcending the realm of technology. It is not, for instance, sufficient to show that the message matches a digital signature signed with the sender's private key, and thus only the sender could have sent the message and nobody else could have altered it in transit. The alleged sender could in return demonstrate that the digital signature algorithm is vulnerable or flawed, or allege or prove that his signing key has been compromised. The fault for these violations may or may not lie with the sender himself, and such assertions may or may not relieve the sender of liability, but the assertion would invalidate the claim that the signature necessarily proves authenticity and integrity and thus prevents repudiation.

Electronic commerce uses technology such as digital signatures and public key encryption to establish authenticity and non-repudiation.

Security policy of information security
Security policy is a definition of what it means to be secure for a system, organization or other entity. For an organization, it addresses the constraints on behavior of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls. For systems, the security policy addresses constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access to data by people.

Significance of security policy
If it is important to be secure, then it is important to be sure all of the security policy is enforced by mechanisms that are strong enough. There are many organized methodologies and risk assessment strategies to assure completeness of security policies and assure that they are completely enforced. In complex systems, such as information systems, policies can be decomposed into sub-policies to facilitate the allocation of security mechanisms to enforce sub-policies. However, this practice has pitfalls. It is too easy to simply go directly to the sub-policies, which are essentially the rules of operation and dispense with the top level policy. That gives the false sense that the rules of operation address some overall definition of security when they do not. Because it is so difficult to think clearly with completeness about security, rules of operation stated as "sub-policies" with no "super-policy" usually turn out to be rambling rules that fail to enforce anything with completeness. Consequently, a top-level security policy is essential to any serious security scheme and sub-policies and rules of operation are meaningless without it.

Computer security policy
A computer security policy defines the goals and elements of an organization's computer systems. The definition can be highly formal or informal. Security policies are enforced by organizational policies or security mechanisms. A technical implementation defines whether a computer system is secure or insecure. These formal policy models can be categorized into the core security principles of: Confidentiality, Integrity and Availability. For example the Bell-La Padula model is a confidentiality policy model, whereas Biba model is an integrity policy model.

Information protection policy
Information protection policy is a document which provides guidelines to users on the processing, storage and transmission of sensitive information. Main goal is to ensure information is appropriately protected from modification or disclosure. It may be appropriate to have new employees sign policy as part of their initial orientation. It should define sensitivity levels of information.

- Should define who can have access to sensitive information.
- Should define how sensitive information is to be stored and transmitted (encrypted, archive files, unencoded, etc.).
- Should define on which systems sensitive information can be stored.
- Should discuss what levels of sensitive information can be printed on physically insecure printers.
- Should define how sensitive information is removed from systems and storage devices.
- Should discuss any default file and directory permissions defined in system-wide configuration files.

REFERENCES

[1]http://www.analytix.co.za/Portals/0/Diagrams/Training---Information-Management-Diagram.jpg. | [2] http://en.wikipedia.org/wiki/Asset_(computing) | [3] en.wikipedia.org /wiki/ Information_security_management_system | [4] www.barrick.com/files/security/Barrick-Security-Management-System.pdf. | [5] ww.infosec.gov.hk/english/technical/files/overview.pdf |