A Brief Survey Of Importance Of Information Security

Ms. Juveria
Assistant Professor
COMM-IT Career Academy (Affiliated to GGSIP University)

Abstract - Information security now a day becomes an important entity for several organizations due to the trends in information transfer through a vulnerable world. This becomes more important to remain aware and to apply Information Security Risk Management (ISRM). However, there are several ISRM methods that are available, most of the ISRM methods prescribe a similar process. However, with the amount, diversity and variety of information available, researchers can easily deflect with grown information. This paper presents a brief description of the attributes of information security (Availability, Confidentiality and Integrity). The paper highlights the fundamental objectives of information security. The paper presents an in-depth explanation of the importance of attributes of information security. The paper also explains importance of the attributes of information security in different situations or cases. The paper also gives a brief description to secure information from unauthorized access. The paper also describes the key components for implementing Information Security Program (ISP).

Keywords - Information Security, Availability, Confidentiality, Integrity, CIA Triad, Information Security Management (ISM), Information Security Program (ISP)

Introduction

Information security (InfoSec) protects information from unauthorized access to avoid identity theft and to protect privacy. Information Security refers to the processes which are designed to protect confidential and sensitive information from unauthorized access or use. Information security can be assured in various ways, including policies, procedures, software programs, hardware etc. Information security is required to protect sensitive information of an organization.

Attributes of Information Security:

Information Security has three attributes: Confidentiality, integrity, and availability. These attributes play important role in an information security program. Confidentiality, Integrity, and Availability (CIA) are the most important pillars of Information Security.

CIA Triad:

Information security focuses on the balanced protection of the confidentiality, integrity and availability of data also known as the CIA triad. The CIA triad of confidentiality, integrity, and availability is the heart and soul of information security. In CIA triad, confidentiality, integrity and availability are the basic goals of information security. The concepts of CIA triad must always be part of the core objectives of information security efforts.

CIA Triad

Confidentiality:

Confidentiality basically is the protection of information from unauthorized access. Confidentially is a component of privacy that implements to protect our data from unauthorized access. For example, electronic data being compromised include laptop theft, password theft, or sensitive emails being sent to the unauthorized users. For example, if we want to maintain confidentiality for a computer file so that only authorized users can access it, while unauthorized users are not able to access it. Confidentiality relates to information security because information security requires access control.

Integrity:

Integrity means maintaining and assuring the accuracy and completeness of information. Integrity of information refers to protecting information from being modified by unauthorized users. This means that data cannot be modified in an unauthorized manner. For example, failure of integrity is when you try to connect to a website and a malicious attacker between you and the website redirects your traffic to a different website. In this case, the site you are directed to is not genuine.

Availability:

Availability, means ensuring timely and consistent access to, and use of information. For any information system to serve its purpose, the information must be available when it is required. This means that the computing systems must be 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. Ensuring the availability involvement for preventing denial-of-service attacks, such as a flood of incoming messages to the target system, essentially forcing it to shut down. Availability can be viewed as one of the most important attribute of information security.

Importance of Attributes of Information Security in Different Situations or Cases:

The following are the situations or cases where one goal of the CIA triad is highly important while other goals are less important:

Confidentiality: Confidentiality means to protect the information from unauthorized use. This attributes emphasizes on the need for information protection. Confidentiality requires measures to ensure that only authorized users are allowed to access the information. In some cases, confidentiality is more important than the other two attributes. For example, information confidentiality is more important than other goals in case of proprietary information of a company. The confidentiality is more important when the information is concerned about the records of people's personal activities. To guarantee confidentiality in information security, a medium of transferring information must be properly monitored and controlled to prevent unauthorized access.

Integrity: Integrity of information refers to protecting information from being modified by unauthorized users. CIA triad goal of integrity is very very important compared to the other goals in some cases of financial information. Any change in financial records leads to issues in accuracy, consistency and value of the information. In the banks integrity of financial records of their customers is more important, with confidentiality having only second priority. To guarantee integrity, information must be protected from unauthorized modification or destruction.

Availability: Availability refers to ensuring that authorized users are able to access the information when needed. CIA triad goal of availability is more important than the other goal when government-generated online press releases are involved. Press releases are generally for public consumption. For them, the information they contain should be available to the public. Thus, confidentiality is not of concern. Integrity has only second priority. In a CIA triad, to guarantee availability of information in press releases, government ensures that their websites and systems have minimal downtime.

Information Security Management (ISM):

Information security management (ISM) describes controls that an organization needs to implement to ensure that it is sensibly protecting the confidentiality, availability, and integrity of assets from unauthorized access. The goal of Information Security Management System (ISMS) is to protect information of organization, both online and in person. The implementation of ISMS will vary from organization to organization, some underlying principles are there that all ISMS abide, in order to protect an organization's information assets.

Information Security Risk Management (ISRM):

Risk management is an activity directed towards assessment and monitoring of risks to an organization. Information security risk management is a subset of the enterprise risk management process, which includes the assessment of information security risks to the institution as well as its purpose is to take appropriate management actions and established priorities for managing and implementing controls to protect against those risks.

It can be broadly divided into two components:

- Risk assessment
- Risk treatment

Risk assessment: Risk assessment identifies and prioritizes risks against criteria for risk acceptance and objectives relevant to the organization. The assessment results guide the determination of appropriate management action and for implementing controls selected to protect against these risks. The assessment should include both a systematic approach to estimate the magnitude of risks and a process for comparing estimated risks against risk criteria to determine the significance of the risks.

Risk treatment: Risk treatment is the next step after risk assessment. For each and every risk identified during a risk assessment, a risk treatment decision needs to be made. Some of the possible options for risk treatment include: knowingly and objectively accepting risks, providing clearly the organization's policy and criteria for risk acceptance, applying suitable controls to reduce the risks etc.

Information Security Program (ISP):

An information security program helps organizations to secure their infrastructure, especially if regulations mandate how you must protect sensitive data. Regardless of the size of your organization, an information security program is a critical component of any organization. A good information security program consists of a set of information security policies and procedures, which is the cornerstone to any information security program.

Key Components for implementing Information Security Program (ISP):

In order to achieve the strategic, tactical and operational goals, the following are key components to successfully implementing an Information Security Program**:**

1. Focus on the Information Security Program as a whole
2. Align your security program with your organization's mission and business objectives
3. Implement meaningful and enforceable Information Security policies and procedures
4. Develop a security risk management program
5. Apply defense-in-depth measures: Assess the security controls to identify and manage risk
6. Establish a culture of security
7. Measure your Information Security Program by developing meaningful metrics
8. Develop and implement an Incident Response Plan
9. Continuous monitoring
10. Review your plan at least annually

Conclusion: Now a day's information security becomes an important unit of any organization. Information security protects information from unauthorized access. Confidentiality, integrity and availability (CIA) are the unifying attributes of an information security. Banks and other such organizations are vulnerable with information security. In order to achieve information security, we must follow the key components to successfully implement an Information Security Program (ISP). As we see organizations adapt changing business environments, they should also adapt Information Security Management Systems (ISMS) for changing technological advances and new organizational information.

References:

- Information Security: Principles and Practice,2nd Edition
  By: Mark S. Merkow
- Computer and Information Security: Handbook
  By: John R. Vacca
- Principles of Information Security
  By: Michael E. Whitman
- Basics of Information Security
  By: Jason Andress