Chapter 1

Information Assurance and Security

Introduction

What is Information Assurance?

Information Assurance is defined as the set of measures intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. These measures are planned and executed by the Information Assurance Directorate (IAD) of the National Security Agency/Central Security Service (NSA/CSS).

Information assurance (IA) is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes.

Information assurance includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data. It uses physical, technical and administrative controls to accomplish these tasks. While focused predominantly on information in digital form, the full range of Information assurance encompasses not only digital but also analog or physical form. These protections apply to data in transit, both physical and electronic forms as well as data at rest in various types of physical and electronic storage facilities. Information assurance as a field has grown from the practice of information security.

Why Information Assurance is needed?

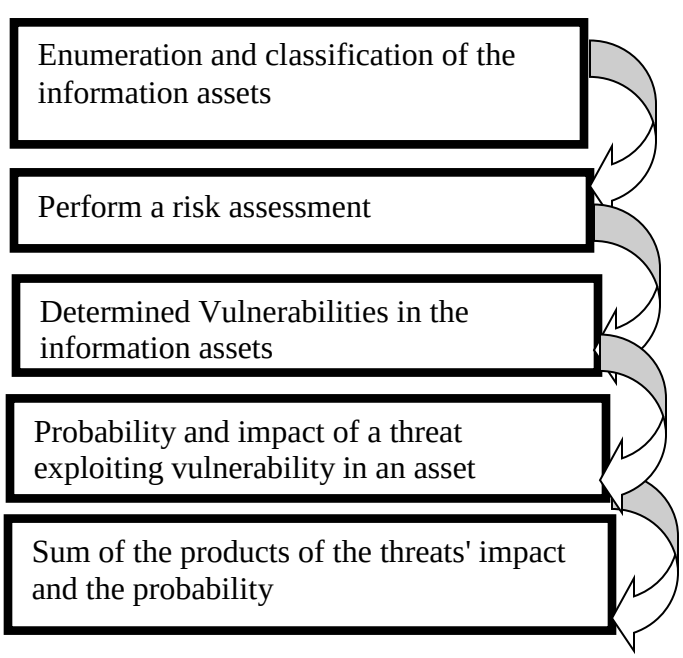
The mission has evolved through three very distinct stages: Communications Security (COMSEC), Information Systems Security (INFOSEC) and Information Assurance (IA). Post WWI and the Korean War, COMSEC efforts focused primarily on cryptography (i.e., designing and building encryption devices to provide confidentiality for information). The introduction and widespread use of computers created new demands to protect information exchanges between interconnected computer systems. This demand created the Computer Security (COMPUSEC) discipline. With the introduction of COMPUSEC came the recognition that stand-alone COMSEC and stand-alone COMPUSEC could not protect information during storage, processing or transfer between systems. This recognition gave rise to the term INFOSEC and the information protection mission took on a broader perspective. IA emerged and focused on the need to protect information during transit, processing, or storage within complex and/or widely dispersed computers and communication system

networks. IA includes a dynamic dimension where the network architecture is itself a changing environment, including the information protection mechanisms that detect attacks and enable a response to those attacks.
Information assurance is the process of adding business benefit through the use of IRM (Information Risk Management) which increases the utility of information to authorized users, and reduces the utility of information to those unauthorized. It is strongly related to the field of information security, and also with business continuity.

IA practitioners consider corporate governance issues such as privacy, regulatory and standards compliance, auditing, business continuity, and disaster recovery as they relate to information systems.
Therefore, IA is best thought of as a superset of information security (i.e. umbrella term), and as the business outcome of Information Risk Management.

Information assurance process

1. Enumeration and classification of the information assets to be protected.
2. Next, the IA practitioner will perform a risk assessment for those assets.
3. Vulnerabilities in the information assets are determined in order to enumerate the threats capable of exploiting the assets.
4. Consider the probability of a threat exploiting vulnerability in an asset
5. Impact of a threat exploiting vulnerability in an asset, with impact usually measured in terms of cost to the asset's stakeholders.
6. The sum of the products of the threats' impact and the probability of their occurring is the total risk to the information asset.



With the risk assessment complete, the IA practitioner then develops **a risk management plan.**

Risk management plan proposes countermeasures

1. Detection,
2. Accepting
3. Mitigating/ justify
4. Response to threats.
5. Eliminating
6. Considers prevention
7. Transferring the risks,

What is countermeasure?

In computer security a **countermeasure** is an action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

It include technical tools such as firewalls and anti-virus software, policies and procedures requiring such controls as regular backups and configuration hardening, employee training in security awareness, or organizing personnel into dedicated **computer emergency response team** (CERT) or **computer security incident response team** (CSIRT)**.** The cost and benefit of each countermeasure is carefully considered. Thus, the IA practitioner does not seek to eliminate all risks, were that possible, but to manage them in the most cost-effective way.

After the risk management plan is implemented, it is tested and evaluated, often by means of formal audits. The IA process is an iterative one, in that the risk assessment and risk management plan are meant to be periodically revised and improved based on data gathered about their completeness and effectiveness.

Five Information Assurance pillars

The five information assurance (IA) pillars are availability, integrity, authentication, confidentiality, and non-repudiation. These pillars and any measures taken to protect and defend information and information systems, to include providing for the restoration of information systems, constitute the essential underpinnings for ensuring trust and integrity in information systems.

The cryptologic components of information assurance primarily address the last four pillars of integrity, authentication, confidentiality, and non-repudiation. These pillars are applied in accordance with the mission needs of particular organizations.

1. integrity, which means protecting against improper information modification or damage, and includes ensuring information non repudiation and authenticity;
2. confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;
3. availability, which means ensuring timely and reliable access to and use of information

Information Assurance strategy

- Cyber security awareness and education;
- Strong cryptography;
- Good security-enabled commercial information technology;
- An enabling global Security Management Infrastructure; and
- A civil defense infrastructure equipped with an attack sensing and warning capability and coordinated response mechanism

Difference between information protection and information assurance in Data Protection

- ✓ Information Assurance (AI): Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
- ✓ Information protection (or information security as defined by the NIST): The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide

Information security

The end of the 20th century and early years of the 21st century saw rapid advancements in telecommunications, computing hardware and software, and data encryption. The availability of smaller, more powerful and less expensive computing equipment made electronic data processing within the reach of small business and the home user. These computers quickly became interconnected through the Internet.

The rapid growth and widespread use of electronic data processing and electronic business conducted through the Internet, along with numerous occurrences of international terrorism, fueled the need for better methods of protecting the computers and the information they store, process and transmit.

The academic disciplines of computer security and information assurance emerged along with numerous professional organizations – all sharing the common goals of ensuring the security and reliability of information systems.

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...) Two major aspects of information security are:

- **IT security**: Sometimes referred to as computer security, Information Technology Security is information security applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory (even a calculator). IT security specialists are responsible for keeping all of the technology within the company secure from malicious cyber-attacks that often attempt to breach into critical private information or gain control of the internal systems.
- **Information assurance**: The act of ensuring that data is not lost when critical issues arise. These issues include but are not limited to: natural disasters, computer/server malfunction, physical theft, or any other instance where data has the potential of being lost. Since most information is stored on computers in our modern era, information assurance is typically dealt with by IT security specialists. One of the most common methods of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arises.

Governments, military, corporations, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers.

Functionalities of Information Assurance and Security:

1. "Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved."
2. "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."
3. "Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)."
4. "Information Security is the process of protecting the intellectual property of an organization."

5. "...information security is a risk management discipline, whose job is to manage the cost of information risk to the business."
6. "A well-informed sense of assurance that information risks and controls are in balance."
7. "Information security is the protection of information and minimises the risk of exposing information to unauthorised parties."

Computer security

The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users. The term computer system security means the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals and unplanned events respectively.

The strategies and methodologies of computer security often differ from most other computer technologies because of its somewhat elusive objective of preventing unwanted computer behavior instead of enabling wanted computer behavior.

Computer Security - generic name for the collection of tools designed to protect data and to thwart hackers

Network Security - measures to protect data during their transmission

Internet Security - measures to protect data during their transmission over a collection of interconnected networks

Why Security?

Computer security is required because most organizations can be damaged by Virus software or intruders. There may be several forms of damage which are obviously interrelated. These include:

- Damage or destruction of computer systems, and internal data.
- Loss of sensitive information to hostile parties. Use of sensitive information to steal items of monitory value.
- Use of sensitive information against the organization's customers which may result in legal action by customers against the organization and loss of customers.
- Damage to the reputation of an organization.
- Monitory damage due to loss of sensitive information, destruction of data, hostile use of sensitive data, or damage to the organization's reputation.

Principles of Security

These three concepts form what is often referred to as the **CIA triad** (Figure 1). The three concepts embody the fundamental security objectives for both data and for information and computing services. FIPS PUB 199 provides a useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category:

These three concepts such as Confidentiality, Integrity and Availability form, what is often referred to as the **CIA triad** (Figure 1)

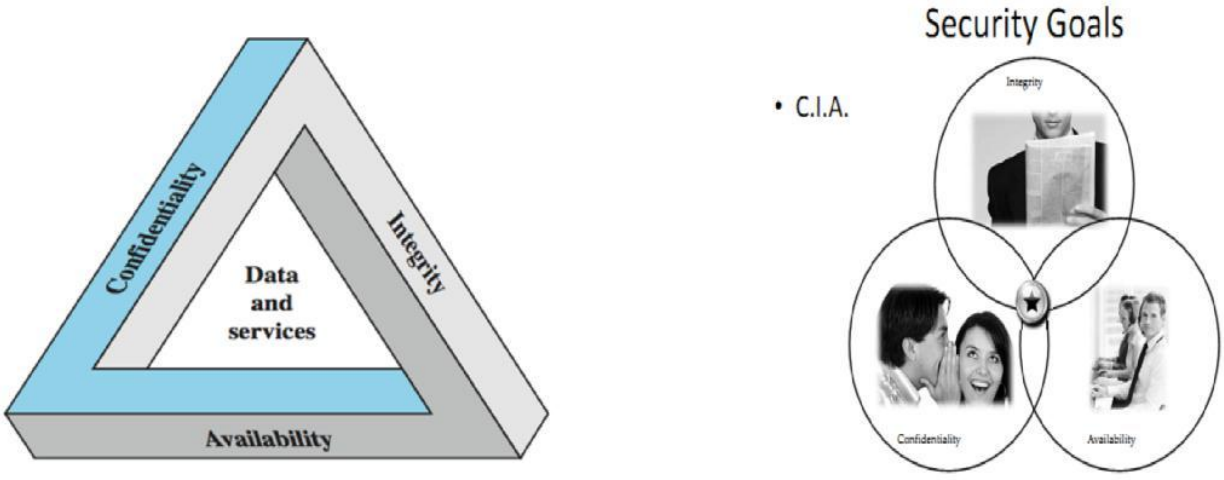


Fig 1: Key Security Concepts

The three concepts embody the fundamental security objectives for both data and for information and computing services. FIPS PUB 199 provides a useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category:

1. Confidentiality:

- **Confidentiality** is a set of rules that limits access to information.
- Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems.
- Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it.
- Training can help familiarize authorized people with risk factors and how to guard against them. Further aspects of training can include strong passwords and password-related best practices and information about social engineering methods.

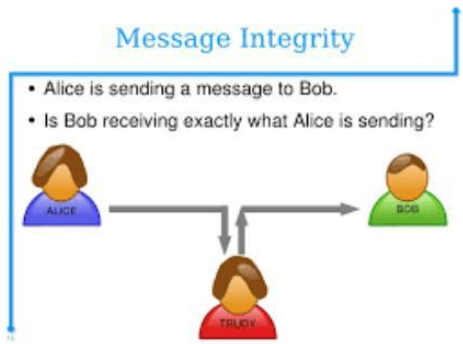
The terms privacy and secrecy are sometimes used to distinguish between the protection of personal data **(privacy)** and the protection of data belonging to an organization **(secrecy).**

For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information. “Prevention of unauthorized disclosure of information”.

2. Integrity:



- Integrity is the assurance that the information is trustworthy and accurate.
- **Integrity** involves maintaining the **consistency, accuracy, and trustworthiness** of data over its entire life cycle.
- Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality).
- This goal defines how we avoid our data from being altered. MiTM (Man in the middle attacks) is the example threat for this goal.

Integrity is about making sure that everything is as it is supposed to be, and in the context of computer security, the prevention of unauthorized modification of information.

However, additional qualifications like “being authorized to do what one does” or following the correct procedures” have also been included under the term integrity, so that users of a system, even if authorized, are not permitted to modify data items in such a way that assets or accounting records of the company are lost or corrupted.

In Computer security, integrity means that data cannot be modified undetectably.

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information. Prevention of unauthorized modification of information.

3. Availability:

- It means that assets are accessible to authorized parties at appropriate times.
- Availability is very much a concern beyond the traditional boundaries of computer security. We want to ensure that a malicious attacker cannot prevent legitimate users from having reasonable access to their systems.

INFORMATION SECURITY

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.

These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration.

- Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.
- Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.
- Information assurance focuses on the reasons for assurance that information is protected, and is thus reasoning about information security.

What Is Enterprise security?

Enterprise security is about building systems to remain dependable in the face of malice, error, or mischance. As a discipline, it focuses on the tools, processes, and methods needed to design, implement, and test complete systems, and to adapt existing systems as their environment evolves.

Enterprise security requires cross-disciplinary expertise, ranging from cryptography and computer security through hardware tamper-resistance and formal methods to a knowledge of economics, applied psychology, organizations and the law. System engineering skills, from business process analysis through software engineering to evaluation and testing, are also important; but they are not sufficient, as they deal only with error and mischance rather than malice.

Many security systems have critical assurance requirements.

A Enterprise Security Analysis Framework

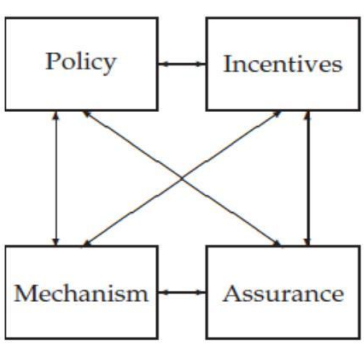


Figure 1: Enterprise Security Analysis Framework

Good Enterprise security requires four things to come together.

1. **Policy**: what you're supposed to
2. **Mechanism**: the ciphers, access controls, hardware tamper-resistance and other machinery that you assemble in order to implement the policy.
3. **Assurance**: the amount of confidence you can place on each particular mechanism.
4. **Incentive**: the motive that the people guarding and maintaining the system have to do their job properly, and also the motive that the attackers have to try to defeat your policy. All of these interact

Enterprise Security within an Enterprise Architecture Context:

Many of the terms used in Enterprise security are straightforward, but some are misleading or even controversial. There are more detailed definitions of technical terms in the relevant chapters, which you can find using the index.

The first thing we need to clarify is what we mean by system. In practice, this can denote:

1. a product or component, such as a cryptographic protocol, a smartcard or the hardware of a PC;
2. a collection of the above plus an operating system, communications and other things that go to make up an organization's infrastructure;
3. the above plus one or more applications (media player, browser, word processor, accounts / payroll package)
4. any or all of the above plus IT staff;
5. any or all of the above plus internal users and management;
6. any or all of the above plus customers and other external users.

Enterprise Security Architecture: Establishing the Business Context

A **business-driven approach** to enterprise security architecture means that security is about enabling the objective of an organization by controlling operational risk. This business-driven approach becomes a key differentiator to existing security practices that are focused solely on identifying threats to an enterprise and technical vulnerabilities in IT infrastructure, and subsequently implementing controls to mitigate the risks introduced.

A purely **threat-based approach** to risk management fails to enable effective security and business operations. The term security will carry very different meanings to different organizations.

For example, consider security as it relates to a **military organization** and security related to an **online retailer** that processes credit card information.

Cyber Defense

Definition - What does Cyber Defense mean?

Cyber defense is a computer network defense mechanism which includes response to actions and critical infrastructure protection and information assurance for organizations, government entities and other possible networks.

Cyber defense focuses on

1. preventing, detecting and providing timely responses to attacks or threats
2. Prevent with the growth in volume as well as complexity of cyber-attacks,
3. It is essential for most entities in order to protect sensitive information as well as to safeguard assets.
4. It helps in devising and driving the strategies necessary to counter the malicious attacks or threats.
5. It reducing the appeal of the environment to the possible attackers,
6. Cyber defense also carries out technical analysis to identify the Threat
7. It helps in enhancing the security strategy utilizations and resources in the most effective fashion.
8. Cyber defense also helps in improving the effectiveness of the security resources and security expenses, especially in critical locations.
9. Cyber Defense protects your most important business assets against attack.