**CYBER SECURITY NOTES**

**UNIT 1**

 **STUTI PANDEY**

 **CSE DEPTT.**

**Data and information**

**Data** is raw unprocessed facts and figures that have no context orpurposeful meaning and **Information** is processed data that has meaning and is presented in a context.

For example, a computer operator may enter 36.41, which is data, because we do not know why or in what context it is being used. However, if this number then appears on a bill to show that you owe a company £36.41 for goods received then this data has changed into information, because it has acquired a context (it’s a bill) and meaning.

The figures 36.41 will be held as binary data on some media such as a hard disk. It is the software which accesses this data and displays it in its context. It may also have some structure, if it is held in a program like a database for example, and a database will also give it structure. So, it is the software which turns the figures from data into information and gives them meaning.

**Knowledge**

Humans have an endless thirst for knowledge, but how do we obtain knowledge? We can read books and magazines, study course materials, and of course we can gain knowledge from watching TV and listening to the radio. The knowledge about the weekend’s sports matches can mean as much to one person as the latest advances in rocket science does to another.

We tend to gain knowledge from information and we use that information to make decisions.

Knowledge can be split into two categories: *explicit* and *tacit*. *Explicit* knowledge is rules or processes or decisions that can berecorded either on paper or in an information system. *Tacit* knowledge exists inside the minds of humans and is harder to record. It tends to be created from someone’s experiences, so again it is based on a set of rules or experiences.

**Metadata**

Metadata can be thought of as data that describes data. It may have been introduced to you in the Database Unit where it is defined as a data dictionary. This is one example, but other formats of metadata exist. It may be the card-index system used by libraries before computerisation, where each card told you the author, title and location of the book. It can also be thought of as data about documents or files stored on the computer. The computer keeps a file on its hard disk where it records information about each and every file on the computer. This includes information such as when the file was created or modified; who created it; the size of the file; the file type it is. This master or directory file is an example of metadata.

**Characteristics of information**

Good information is that which is used and which creates value. Experience and research shows that good information has numerous qualities.

Good information is **relevant** for its purpose, sufficiently **accurate** for its purpose, **complete** enough for the problem, **reliable** and **targeted** to the right person. It is also communicated **in time** forits purpose, contains the right level of detail and is communicated by an appropriate channel, i.e. one that is **understandable** to the user.

**Information System**

**Information system** is an academic study of **systems** with a specific reference to **information** and the complementary networks of hardware and software that people and organizations use to collect, filter, process, create and also distribute data.

**OR**

An **information system** (**IS**) is any organized system for the collection, organization, storage and communication of information. More specifically, it is the study of complementary networks that people and organizations use to **collect**, **filter**, **process**, **create** and **distribute data**.

A computer information system is a system composed of people and computers that processes or interprets information. The term is also sometimes used in more restricted senses to refer to only the software used to run a computerized database or to refer to only a computer system.

An emphasis is placed on an Information System having a definitive Boundary, Users, Processors, Stores, Inputs, Outputs and the aforementioned communication networks.

Any specific information system aims to support operations, management and [decision-making](https://en.wikipedia.org/wiki/Decision-making).An information system is the [information and communication technology](https://en.wikipedia.org/wiki/Information_and_communication_technology) (ICT) that an organization uses, and also the way in which people interact with this technology in support of business processes

**Types of information Systems**

The "classic" view of Information systems found in the 1980s was of a pyramid of systems that reflected the hierarchy of the organization, usually [transaction processing systems](https://en.wikipedia.org/wiki/Transaction_processing_systems) at the bottom of the pyramid, followed by [management information systems](https://en.wikipedia.org/wiki/Management_information_systems), [decision support systems](https://en.wikipedia.org/wiki/Decision_support_systems), and ending with [executive information systems](https://en.wikipedia.org/wiki/Executive_information_systems) at the top. Although the pyramid model remains useful, since it was first formulated a number of new technologies have been developed and new categories of information systems have emerged, some of which no longer fit easily into the original pyramid model.

An information system is a group of interrelated components that work to carry out input, processing, storage, output and control actions in order to convert data into information that can be used to support forecasting, planning, control, coordination, decision making and operational activities in an organisation.

There are several categories of information system:

* Data Processing Systems (DPS)
* Management Information Systems (MIS)
* Decision Support Systems (DSS)
* Executive Information System (EIS).

This table shows how they fit into the categories of strategic, tactical, and operational information systems:

|  |  |
| --- | --- |
| **Organisation level** | **Type of information system** |
|  |  |
| Strategic | Executive information system |
|  |  |
| Tactical | Decision support system |
|  |  |
|  | Management information system |
|  |  |
| Operational | Data processing system |
|  |  |



**Fig. 1- A Four Level**

**Data processing systems**

Commercial computing systems were first developed in the 1950s and 60s, initially by what can only be called enthusiasts consisting of businessmen with a vision.

These systems were data processing systems that either replaced the manual clerical procedures currently in use (like bank records), or in new areas where humans were unable to perform the calculations involved due to their complexity.

A Data Processing System is sometimes referred to as a Transaction Processing System (TPS), because it deals with the day-to-day transactions of an organisation. Examples include systems for accountancy, invoicing, stock control and data entry. For example, a clerk processing a customer order needs to know whether the item is in stock, what the price of the item is, as well as customer details including name and address.

Another example is each item sold in a supermarket. For each item the bar code would be scanned and used to find the name and the price of the product and then the price used to calculate the total bill for a customer. This type of event would be stored in the supermarket’s transaction file for each day’s business.

Data processing systems are usually tools used at the operational level of an organisation, since most organisations at an operational level produce large amounts of data from the events that contribute to their running.

Another simpler example of a DPS, within a school context, is the gathering of pupil attendance records. Usually some attendance data is gathered for pupils in a school, in the morning and afternoon. This data is then input into the attendance information system. It can be used to calculate pupil, class, and year-group attendance percentages. Pupil support staff enquiring about pupil illness or poor attendance can also use the information produced by this system.

**Management information systems**

An MIS is a system that converts data from internal and external sources into information, managers at different levels of an organisation. The information can contribute to effective decision making or planning to be carried out.

The source of data for an MIS usually comes from numerous databases. These databases are usually the data storage for Data Processing Systems.

MIS summarise and report on the organisation’s basic operations. The basic data from the DPS is condensed and is usually presented in long reports that are produced on a regular basis.

MIS produce reports for managers interested in historic trends on a weekly, monthly and yearly basis (not on the day-to-day activities of the DPS). The information in these reports provides answers to routine pre-defined questions. An example from a supermarket will provide reports that show the sales figures for each department each day for a week, with weekly totals, monthly totals, comparisons with last month and the corresponding month last year. Once the information is in the system many reports can be extracted.

These systems are generally not very flexible and have little analytical capability. Most MIS use simple routines such as summaries and comparisons as opposed to sophisticated mathematical models or statistical techniques.

**Decision support systems**

A DSS provides information and models in a form to help tactical and strategic decision-making. DSS support management decision-making by integrating:

* company performance data
* business rules in a decision table
* analytical tools and models for forecasting and planning
* a simple user interface to query the system.

DSS are particularly useful when making ad-hoc, one-off decisions. These types of decisions tend to be unstructured and irregular.

DSS enable a manager to explore a range of alternatives under a variety of conditions. For example, a manager may wish to know the effects on profits if sales increase and costs decrease.

**Executive information system**

An EIS provides senior managers with a system to assist in taking strategic and tactical decisions. Its purpose is to analyse, compare and identify trends to help the strategic direction of the organisation.

EIS address unstructured decisions and create a generalised computing and communications environment, rather than providing any fixed application or specific capability. Such systems are not designed to solve specific problems, but to tackle a changing array of problems.

EIS are designed to incorporate data about external events, such as new tax laws or competitors, and also draw summarised information from internal MIS and DSS. These systems filter, compress, and track critical data; emphasising the reduction of time and effort required to obtain information useful to strategic management. They employ advanced graphics software to provide highly visual and easy-to-use representations of complex information and current trends, but they tend not to provide analytical model

EIS allow the user to look at specific data that has been summarised from lower levels within the organisation and then *drill down* to increase the level of detail, which is provided by theinformation systems in different areas. This is an example of data warehouse analysis, which we will discuss later.

**EIS**

|  |  |
| --- | --- |
| **MIS** | **DSS** |

**DPS**

 ***Interrelationships between Information systems***

**Expert systems**

An expert system is a computer program that tries to emulate human reasoning. It does this by combining the knowledge of human experts and then, following a set of rules, it draws inferences.

An expert system is made up of three parts: a knowledge base; an inference engine; a user interface.

The *knowledge base* stores all of the facts, rules and information needed to represent the knowledge of the expert. The *inference* *engine* is the part of the expert system that interprets the rules andfacts using backward and forward chaining to find solutions to user queries. The *user interface* allows the user to enter new knowledge and query the system.

***Reasons for expert systems in business:***

* To store information in an active form as organisational memory, creating an organisational knowledge base that many employees can examine and preserving expertise that might be lost when an acknowledged expert leaves the organisation.
* To create a mechanism that is not subject to human feelings, such as fatigue and worry. This may be especially useful when jobs may be environmentally, physically or mentally dangerous to humans. These systems may also be useful advisers in times of crisis.
* To enhance the organisation’s knowledge base by generating solutions to specific problems that are too substantial and complex to be analysed by human beings in a short period of time

**Development of Information Systems**

Information technology departments in larger organizations tend to strongly influence the development, use, and application of information technology in the organizations. A series of methodologies and processes can be used to develop and use an information system. Many developers now use an engineering approach such as the [system development life cycle](https://en.wikipedia.org/wiki/System_development_life_cycle) (SDLC), which is a systematic procedure of developing an information system through stages that occur in sequence. Recent research aims at enabling and measuringthe ongoing, collective development of such systems within an organization by the entirety of human actors themselves. An information system can be developed in house (within the organization) or outsourced. This can be accomplished by outsourcing certain components or the entire system. A specific case is the geographical distribution of the development team ([offshoring](https://en.wikipedia.org/wiki/Offshoring), [global information system](https://en.wikipedia.org/wiki/Global_information_system)).

A computer-based information system is a technologically implemented medium for:

* recording, storing, and disseminating linguistic expressions,
* as well as for drawing conclusions from such expressions.

[Geographic information systems](https://en.wikipedia.org/wiki/Geographic_information_system), land information systems, and disaster information systems are examples of emerging information systems, but they can be broadly considered as spatial information systems. System development is done in stages which include:

* Problem recognition and specification
* Information gathering
* Requirements specification for the new system
* System design
* System construction
* System implementation
* Review and maintenance.

# Types of Software developing life cycles (SDLC)

* Waterfall Model
* V-Shaped Model·
* Evolutionary Prototyping Model
* Spiral Method ([SDM](http://en.wikipedia.org/wiki/Software_development_methodology))
* Iterative and Incremental Method
* Extreme programming ([Agile development](http://en.wikipedia.org/wiki/Agile_software_development))

## Waterfall Model

##### **Description**

The waterfall Model is a linear sequential flow. In which progress is seen as flowing steadily downwards (like a waterfall) through the phases of software implementation. This means that any phase in the development process begins only if the previous phase is complete. The waterfall approach does not define the process to go back to the previous phase to handle changes in requirement. The waterfall approach is the earliest approach that was used for software development.

##### **The usage**

Projects which not focus on changing the requirements, for example, projects initiated from request for proposals ([RFPs](http://en.wikipedia.org/wiki/Request_for_proposal))

##### **Advantages and Disadvantages**

|  |  |
| --- | --- |
| **Advantages** | **Disadvantages** |
| · Easy to explain to the user· Structures approach.· Stages and activities are well defined· Helps to plan and schedule the project· Verification at each stage ensures early detection of errors / misunderstanding· Each phase has specific deliverables | · Assumes that the requirements of a system can be frozen· Very difficult to go back to any stage after it finished.· Little flexibility and adjusting scope is difficult and expensive.· Costly and required more time, in addition to detailed plan |



## V-Shaped Model

##### **Description**

It is an extension for waterfall model, Instead of moving down in a linear way, the process steps are bent upwards after the coding phase, to form the typical V shape. The major difference between v-shaped model and waterfall model is the early test planning in v-shaped model.

##### **The usage**

· Software requirements clearly defined and known

· Software development technologies and tools is well-known

##### **Advantages and Disadvantages**

|  |  |
| --- | --- |
| **Advantages** | **Disadvantages** |
| · Simple and easy to use.· Each phase has specific deliverables.· Higher chance of success over the waterfall model due to the development of test plans early on during the life cycle.· Works well for where requirements are easily understood. Verification and validation of the product in early stages of product development | · Very inflexible, like the waterfall model.· Little flexibility and adjusting scope is difficult and expensive.· Software is developed during the implementation phase, so no early prototypes of the software are produced.· Model doesn’t provide a clear path for problems found during testing phases.· Costly and required more time, in addition to detailed plan |



##

## Prototyping Model

##### **Description**

It refers to the activity of creating prototypes of software applications, for example, incomplete versions of the software program being developed. It is an activity that can occur in software development. It used to visualize some component of the software to limit the gap of misunderstanding the customer requirements by the development team. This also will reduce the iterations may occur in waterfall approach and hard to be implemented due to inflexibility of the waterfall approach. So, when the final prototype is developed, the requirement is considered to be frozen.It has some types, such as:

· Throwaway prototyping: Prototypes that are eventually discarded rather than becoming a part of the finally delivered software

· 

**Evolutionary prototyping**: prototypes that evolve into the final system through iterative incorporation of user feedback.



·

 **Incremental prototyping**: The final product is built as separate prototypes. At the end the separate prototypes are merged in an overall design.



**Extreme prototyping**: used at web applications mainly. Basically, it breaks down web development into three phases, each one based on the preceding one. The first phase is a static prototype that consists mainly of HTML pages. In the second phase, the screens are programmed and fully functional using a simulated services layer. In the third phase the services are implemented

##### **The usage**

· This process can be used with any software developing life cycle model. While this shall be focused with systems needs more user interactions. So, the system do not have user interactions, such as, system does some calculations shall not have prototypes.

##### **Advantages and Disadvantages**

|  |  |
| --- | --- |
| **Advantages** | **Disadvantages** |
| · Reduced time and costs, but this can be disadvantage if the developer loses time in developing the prototypes· Improved and increased user involvement | · Insufficient analysis· User confusion of prototype and finished system· Developer misunderstanding of user objectives· Excessive development time of the prototype· Expense of implementing prototyping |

##

## Spiral Method (SDM)



##### **Description**

It is combining elements of both design and prototyping-in-stages, in an effort to combine advantages of top-down and bottom-up concepts. This model of development combines the features of the prototyping model and the waterfall model. The spiral model is favored for large, expensive, and complicated projects. This model uses many of the same phases as the waterfall model, in essentially the same order, separated by planning, risk assessment, and the building of prototypes and simulations.

##### **The usage**

It is used in shrink-wrap large applications and systems which built-in small phases or segments.

##### **Advantages and Disadvantages**

|  |  |
| --- | --- |
| **Advantages** | **Disadvantages** |
| · Estimates (i.e. budget, schedule, etc.) become more realistic as work progresses, because important issues are discovered earlier.· Early involvement of developers· Manages risks and develops system into phases | · High cost and time to reach the final product.· Needs special skills to evaluate the risks and assumptions· Highly customized limiting re-usability |

##

## Iterative and Incremental Method

##### **Description**

It is developed to overcome the weaknesses of the waterfall model. It starts with an initial planning and ends with deployment with the cyclic interactions in between. The basic idea behind this method is to develop a system through repeated cycles (iterative) and in smaller portions at a time (incremental), allowing software developers to take advantage of what was learned during development of earlier parts or versions of the system.

It consists of mini waterfalls



##### **The usage**

It is used in shrink-wrap application and large system which built-in small phases or segments. Also can be used in system has separated components, for example, ERP system. Which we can start with budget module as first iteration and then we can start with inventory module and so forth.

##### **Advantages and Disadvantages**

|  |  |
| --- | --- |
| **Advantages** | **Disadvantages** |
| · Produces business value early in the development life cycle· Better use of scarce resources through proper increment definition· Can accommodate some change requests between increments· More focused on customer value than the linear approaches· Problems can be detected earlier | · Requires heavy documentation· Follows a defined set of processes· Defines increments based on function and feature dependencies· Requires more customer involvement than the linear approaches· Partitioning the functions and features might be problematic· Integration between iteration can be an issue if this is not considered during the development. |

##

## Extreme programming (Agile development)

##### **Description**

It is based on iterative and incremental development, where requirements and solutions evolve through collaboration between cross-functional teams.



##### **The usage**

It can be used with any type of the project, but it needs more involvement from customer and to be interactive. Also, it can be used when the customer needs to have some functional requirement ready in less than three weeks.

##### **Advantages and Disadvantages**

|  |  |
| --- | --- |
| **Advantages** | **Disadvantages** |
| · Decrease the time required to avail some system features.· Face to face communication and continuous inputs from customer representative leaves no space for guesswork.· The end result is the high quality software in least possible time duration and satisfied customer | · Scalability· Skill of the software developers· Ability of customer to express user needs· Documentation is done at later stages· Reduce the usability of components.· Needs special skills for the team. |

**Information Security**

Information Security, sometimes shortened to **InfoSec**, is the practice of defending [information](https://en.wikipedia.org/wiki/Information) from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).

Information security is not a single technology; rather it a strategy comprised of the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. Processes and policies typically involve both physical and digital security measures to protect [data](http://searchdatamanagement.techtarget.com/definition/data) from unauthorized access, use, replication or destruction. Infosec management can include everything from [mantraps](http://whatis.techtarget.com/definition/mantrap-interlocking-door-controller) to [encryption key management](http://searchdatabackup.techtarget.com/definition/encryption-key-management) and [malware](http://searchmidmarketsecurity.techtarget.com/definition/malware) detection.

 **Information Security Policy**

Information security policy is a set of policies issued by an organization to ensure that all information technology users within the domain of the organization or its networks comply with rules and guidelines related to the security of the information stored digitally at any point in the network or within the organization's boundaries of authority.

 **Need for Information Security**

An asset of the system may be lost or become unavailable as an intruder may insert spurious transactions to a network communication system or add records to an existing database, therefore, there is a need of information security.

 The purpose of information security is to devise techniques to prevent the weaknesses from being exploited. There are important aspects of any computer related system namely Confidentiality, Integrity, and Availability

The CIA triad of confidentiality, integrity, and availability is at the heart 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.)

 **Confidentiality - protecting information from being disclosed to unauthorised parties.**

 **Integrity - protecting information from being changed by unauthorised parties.**

 **Availability - to the availability of information to authorised parties only when requested.**

**Confidentiality** is roughly equivalent to [privacy](http://searchcio.techtarget.com/definition/data-privacy-information-privacy). 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: Access must be restricted to those authorized to view the data in question. It is common, as well, for data to be categorized according to the amount and type of damage that could be done should it fall into unintended hands. More or less stringent measures can then be implemented according to those categories.

[**Integrity**](http://searchdatacenter.techtarget.com/definition/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). These measures include file permissions and user [access controls](http://searchsecurity.techtarget.com/definition/access-control). Version control maybe used to prevent erroneous changes or accidental deletion by authorized users becoming a problem. In addition, some means must be in place to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse ([EMP](http://whatis.techtarget.com/definition/electromagnetic-pulse-EMP)) or server [crash](http://whatis.techtarget.com/definition/crash). Some data might include [checksums](http://searchsecurity.techtarget.com/definition/checksum), even [cryptographic checksums](http://searchsecurity.techtarget.com/definition/checksum), for verification of integrity. [Backups](http://searchstorage.techtarget.com/definition/backup) or redundancies must be available to restore the affected data to its correct state.

**Availability i**s best ensured by rigorously maintaining all [hardware](http://searchnetworking.techtarget.com/definition/hardware), performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts. It’s also important to keep current with all necessary system [upgrades](http://searchmobilecomputing.techtarget.com/definition/upgrade).  Providing adequate communication [bandwidth](http://searchenterprisewan.techtarget.com/definition/bandwidth) and preventing the occurrence of [bottlenecks](http://searchenterprisewan.techtarget.com/definition/bottleneck) are equally important. [Redundancy](http://whatis.techtarget.com/definition/redundancy), [failover](http://searchstorage.techtarget.com/definition/failover), [RAID](http://searchstorage.techtarget.com/definition/RAID) even [high-availability clusters](http://searchvirtualstorage.techtarget.com/definition/high-availability-cluster-HA-cluster) can mitigate serious consequences when hardware issues do occur.  Fast and adaptive [disaster recovery](http://whatis.techtarget.com/definition/disaster-recovery) is essential for the worst case scenarios; that capacity is reliant on the existence of a comprehensive disaster recovery plan ([DRP](http://searchenterprisewan.techtarget.com/definition/disaster-recovery-plan)). Safeguards against data loss or interruptions in connections must include unpredictable events such as natural disasters and fire. To prevent data loss from such occurrences, a [backup](http://searchstorage.techtarget.com/definition/backup) copy may be stored in a geographically-isolated location, perhaps even in a fireproof, waterproof safe. Extra security equipment or software such as firewalls and proxy servers can guard against downtime and unreachable data due to malicious actions such as denial-of-service ([DoS](http://searchsoftwarequality.techtarget.com/definition/denial-of-service)) attacks and network intrusions.

****

**Threats to Information Systems**

Computer system threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Most people have experienced software attacks of some sort. Viruses, worms, phishing attacks, and Trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the IT field. Intellectual property is the ownership of property usually consisting of some form of protection. Theft of software is probably the most common in IT businesses today. Identity theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information. Theft of equipment or information is becoming more prevalent today due to the fact that most devices today are mobile. Cell phones are prone to theft and have also become far more desirable as the amount of data capacity increases. Sabotage usually consists of the destruction of an organization′s website in an attempt to cause loss of confidence to its customers. Information extortion consists of theft of a company′s property or information as an attempt to receive a payment in exchange for returning the information or property back to its owner. There are many ways to help protect yourself from some of these attacks but one of the most functional precautions is user carefulness.

**Information Assurance**

Information Assurance (IA) refers to the steps involved in protecting information systems, like computer systems and networks. There are commonly five terms associated with the definition of information assurance:

* Integrity
* Availability
* Authentication
* Confidentiality
* Nonrepudiation

IA is a field in and of itself. It can be thought of as a specialty of Information Technology (IT), because an IA specialist must have a thorough understanding of IT and how information systems work and are interconnected. With all of the threats that are now common in the IT world, such as viruses, worms, phishing attacks, social engineering, identity theft and more, a focus on protection against these threats is required. IA is that focus.

## Information Assurance (IA) Explanation

Essentially, Information Assurance is protecting information systems through maintaining these five qualities of the system.

Integrity involves making sure that an information system remains unscathed and that no one has tampered with it. IA takes steps to maintain integrity, such as having anti-virus software in place so that data will not be altered or destroyed, and having policies in place so that users know how to properly utilize their systems to minimize malicious code from entering them.

Availability is the facet of IA where information must be available for use by those that are allowed to access it. Protecting the availability can involve protecting against malicious code, hackers and any other threat that could block access to the information system.

Authentication involves ensuring that users are who they say they are. Methods used for authentication are user names, passwords, biometrics, tokens and other devices. Authentication is also used in other ways -- not just for identifying users, but also for identifying devices and data messages.

IA involves keeping information confidential. This means that only those authorized to view information are allowed access to it. Information needs to be kept confidential. This is commonly found, for example, in the military, where information is classified or only people with certain clearance levels are allowed access to highly confidential information.

The final pillar is nonrepudiation. This means that someone cannot deny having completed an action because there will be proof that they did it.

**Cyber Security**

**Computer security**, also known as **cybersecurity** or **IT security**, is the protection of [information systems](https://en.wikipedia.org/wiki/Information_system) from theft or damage to the [hardware](https://en.wikipedia.org/wiki/Computer_hardware), the [software](https://en.wikipedia.org/wiki/Software), and to the [information](https://en.wikipedia.org/wiki/Information) on them, as well as from [disruption](https://en.wikipedia.org/wiki/Denial-of-service_attack) o r[misdirection](https://en.wikipedia.org/wiki/Botnet) of the services they provide.

It includes [controlling physical access](https://en.wikipedia.org/wiki/Physical_security) to the hardware, as well as protecting against harm that may come via [network access](https://en.wikipedia.org/wiki/Computer_network), [data](https://en.wikipedia.org/wiki/SQL_injection) and [code injection](https://en.wikipedia.org/wiki/Code_injection),and due to malpractice by operators, whether [intentional](https://en.wikipedia.org/wiki/Insider_threat), [accidental](https://en.wikipedia.org/wiki/Error-tolerant_design), or due to them [being tricked](https://en.wikipedia.org/wiki/Social_engineering_%28security%29) into deviating from secure procedures.

The field is of growing importance due to the increasing reliance on computer systems and the [Internet](https://en.wikipedia.org/wiki/Internet) in most societies, [wireless networks](https://en.wikipedia.org/wiki/Wireless_network) such as [Bluetooth](https://en.wikipedia.org/wiki/Bluetooth) and [Wi-Fi](https://en.wikipedia.org/wiki/Wi-Fi) - and the growth of ["smart" devices](https://en.wikipedia.org/wiki/Smart_devices), including [smartphones](https://en.wikipedia.org/wiki/Smartphone), [televisions](https://en.wikipedia.org/wiki/Television) and tiny devices as part of the [Internet of Things](https://en.wikipedia.org/wiki/Internet_of_Things).

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, the term *security* implies cybersecurity. According to a December 2010 analysis of U.S. spending plans, the federal government has allotted over $13 billion annually to cybersecurity over the next five years.

Ensuring cybersecurity requires coordinated efforts throughout an information system. Elements of cybersecurity include:

* [Application security](http://searchsoftwarequality.techtarget.com/definition/application-security)
* Information security
* Network security
* [Disaster recovery](http://searchenterprisewan.techtarget.com/definition/disaster-recovery-plan) / [business continuity planning](http://searchdisasterrecovery.techtarget.com/definition/business-continuity-action-plan)
* End-user education.

One of the most problematic elements of cybersecurity is the quickly and constantly evolving nature of security risks. The traditional approach has been to focus most resources on the most crucial system components and protect against the biggest known threats, which necessitated leaving some less important system components undefended and some less dangerous risks not protected against. Such an approach is insufficient in the current environment. Adam Vincent, CTO-public sector at Layer 7 Technologies (a security services provider to federal agencies including Defense Department organizations), describes the problem:

*"The threat is advancing quicker than we can keep up with it. The threat changes faster than our idea of the risk. It's no longer possible to write a large white paper about the risk to a particular system. You would be rewriting the white paper constantly..."*

To deal with the current environment, advisory organizations are promoting a more proactive and adaptive approach. The National Institute of Standards and Technology ([NIST](http://searchsoftwarequality.techtarget.com/definition/NIST)), for example, recently issued updated guidelines in its risk assessment framework that recommended a shift toward continuous monitoring and real-time assessments.

**Security Risk Analysis:**

In quantitative risk analysis, an attempt is made to numerically determine the probabilities of various adverse events and the likely extent of the losses if a particular event takes place.

Qualitative risk analysis, which is used more often, does not involve numerical probabilities or predictions of loss. Instead, the qualitative method involves defining the various threats, determining the extent of vulnerabilities and devising countermeasures should an attack occur.

**Risk Assessment**

As part of managing the health and safety of your business, you must control the risks in your workplace. To do this you need to think about what might cause harm to people and decide whether you are taking reasonable steps to prevent that harm.

This is known as risk assessment and it is something you are required by law to carry out. If you have fewer than five employees you don’t have to write anything down. A risk assessment is not about creating huge amounts of paperwork, but rather about identifying sensible measures to control the risks in your workplace. You are probably already taking steps to protect your employees, but your risk assessment will help you decide whether you have covered all you need to.

Think about how accidents and ill health could happen and concentrate on real risks – those that are most likely and which will cause the most harm. For some risks, other regulations require particular control measures. Your assessment can help you identify where you need to look at certain risks and these particular control measures in more detail. These control measures do not have to be assessed separately but can be considered as part of, or an extension of, your overall risk assessment.

**Risk Audit:**

Over the last few years, the need to manage risks has become recognized as an essential part of good corporate governance practice. This has put organizations under increasing pressure to identify all the business risks they face and to explain how they manage them.

In fact, the activities involved in managing risks have been recognized as playing a central and essential role in maintaining a sound system of internal control.

While the responsibility for identifying and managing risks belongs to management, one of the key roles of internal audit is to provide assurance that those risks have been properly managed.

We believe that a professional internal audit activity canbest achieve its mission as a comerstone of governance by positioning its work in the context of the organization’s own risk management framework.

