**CYBER SECURITY**

**(UNIT 3)**

**SUBJECT CODE:AUC-002**

**SEMESTER: 4**

**SESSION: 2016-2017**

**Developing Secure Information System**

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).

**IT security**

Sometimes referred to as [computer security](https://en.wikipedia.org/wiki/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](https://en.wikipedia.org/wiki/Computer) does not necessarily mean a home desktop. A computer is any device with a [processor](https://en.wikipedia.org/wiki/Central_processing_unit) and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the [technology](https://en.wikipedia.org/wiki/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 providing trust of the information, that the Confidentiality, Integrity and Availability (CIA) of the information are not violated. E.g., ensuring that [data](https://en.wikipedia.org/wiki/Data) is not lost when critical issues arise. These issues include, but are not limited to: natural disasters, computer/server malfunction or physical theft. Since most information is stored on computers in our modern era, information assurance is typically dealt with by IT security specialists. A common method of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arise.

### Threats

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.

[Governments](https://en.wikipedia.org/wiki/Governments), [military](https://en.wikipedia.org/wiki/Military), [corporations](https://en.wikipedia.org/wiki/Corporation), [financial institutions](https://en.wikipedia.org/wiki/Financial_institution), [hospitals](https://en.wikipedia.org/wiki/Hospital) and private [businesses](https://en.wikipedia.org/wiki/Businesses) a mass 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](https://en.wikipedia.org/wiki/Computer_network) to other computers.

Should confidential information about a business' customers or finances or new product line fall into the hands of a competitor or a [black hat hacker](https://en.wikipedia.org/wiki/Black_hat_hacker), a business and its customers could suffer widespread, irreparable financial loss, as well as damage to the company's reputation. Protecting confidential information is a business requirement and in many cases also an ethical and legal requirement. Hence a key concern for organizations today is to derive the optimal information security investment. The renowned [Gordon-Loeb Model](https://en.wikipedia.org/wiki/Gordon-Loeb_Model) actually provides a powerful mathematical economic approach for addressing this critical concern.

For the individual, information security has a significant effect on [privacy](https://en.wikipedia.org/wiki/Privacy), which is viewed very differently in different [cultures](https://en.wikipedia.org/wiki/Cultures).

**Application Development Security**

Application security is the use of software, hardware, and procedural methods to protect applications from external threats.  Once an after thought in software design, security is becoming an increasingly important concern during development as applications become more frequently accessible over networks and are, as a result, vulnerable to a wide variety of threats. Security measures built into applications and a sound application security routine minimize the likelihood that unauthorized code will be able to manipulate applications to access, steal, modify, or delete sensitive data.

Actions taken to ensure application security are sometimes called [countermeasure](http://searchsoftwarequality.techtarget.com/definition/countermeasure)s. The most basic software countermeasure is an [application firewall](http://searchsoftwarequality.techtarget.com/definition/application-firewall) that limits the execution of files or the handling of data by specific installed programs. The most common hardware countermeasure is a [router](http://searchnetworking.techtarget.com/definition/router) that can prevent the[IP address](http://searchwindevelopment.techtarget.com/definition/IP-address) of an individual computer from being directly visible on the Internet. Other countermeasures include conventional firewalls, [encryption](http://searchsecurity.techtarget.com/definition/encryption)/decryption programs, anti-virus programs, [spyware](http://searchsecurity.techtarget.com/definition/spyware) detection/removal programs and biometric [authentication](http://searchsecurity.techtarget.com/definition/authentication) systems.

Application security can be enhanced by rigorously defining enterprise assets, identifying what each application does (or will do) with respect to these assets, creating a security profile for each application, identifying and prioritizing potential threats and documenting adverse events and the actions taken in each case. This process is known as [threat modeling](http://searchsecurity.techtarget.com/definition/threat-modeling). In this context, a threat is any potential or actual adverse event that can compromise the assets of an enterprise, including both malicious events, such as a denial-of-service ([DoS](http://searchsecurity.techtarget.com/definition/DOS)) attack, and unplanned events, such as the failure of a storage device.

 terms for application security:

* **Asset**. A resource of value such as the data in a database or on the file system, or a system resource.
* **Threat**. Anything that can exploit a vulnerability and obtain, damage, or destroy an asset.
* [**Vulnerability**](https://en.wikipedia.org/wiki/Vulnerability_%28computing%29). A weakness or gap in security program that can be exploited by threats to gain unauthorized access to an asset.
* [**Attack**](https://en.wikipedia.org/wiki/Attack_%28computing%29) (or exploit). An action taken to harm an asset.
* [**Countermeasure**](https://en.wikipedia.org/wiki/Countermeasure_%28computer%29). A safeguard that addresses a threat and mitigates risk.

**Information Security Governance**

Information governance, or IG, is the set of multi-disciplinary structures, policies, procedures, processes and controls implemented to manage information at an enterprise level, supporting an organization's immediate and future regulatory, legal, risk, environmental and operational requirements. Information governance should determine the balance point between two potentially divergent organizational goals: extracting value from information and reducing the potential risk of information. Information governance reduces organizational risk in the fields of compliance, operational transparency, and reducing expenditures associated with e-discovery and litigation response. An organization can establish a consistent and logical framework for employees to handle data through their information governance policies and procedures. These policies guide proper behavior regarding how organizations and their employees handle electronically stored information ([ESI](https://en.wikipedia.org/wiki/Electronically_stored_information_%28Federal_Rules_of_Civil_Procedure%29)).[[1]](https://en.wikipedia.org/wiki/Information_governance#cite_note-1)[[2]](https://en.wikipedia.org/wiki/Information_governance#cite_note-2)

Information governance encompasses more than traditional [records management](https://en.wikipedia.org/wiki/Records_management). It incorporates [information security](https://en.wikipedia.org/wiki/Information_security) and protection, compliance, [data governance](https://en.wikipedia.org/wiki/Data_governance), [electronic discovery](https://en.wikipedia.org/wiki/Electronic_discovery), [risk management](https://en.wikipedia.org/wiki/Risk_management), privacy, data storage and archiving, [knowledge management](https://en.wikipedia.org/wiki/Knowledge_management), business operations and management, audit, analytics, IT management, [master data management](https://en.wikipedia.org/wiki/Master_data_management), [enterprise architecture](https://en.wikipedia.org/wiki/Enterprise_architecture), [business intelligence](https://en.wikipedia.org/wiki/Business_intelligence), [big data](https://en.wikipedia.org/wiki/Big_data), [data science](https://en.wikipedia.org/wiki/Data_science), and finance.

The five general governance areas are:

1. Govern the operations of the organization and protect its critical assets
2. Protect the organization's market share and stock price (perhaps not appropriate for education)
3. Govern the conduct of employees (educational AUP and other policies that may apply to use of technology resources, data handling, etc.)
4. Protect the reputation of the organization
5. Ensure compliance requirements are met

**Characteristics of effective security governance**

1. It is an institution-wide issue
2. Leaders are accountable
3. It is viewed as an institutional requirement (cost of doing business)
4. It is risk-based
5. Roles, responsibilities and segregation of duties are defined
6. It is addressed and enforced in policy
7. Adequate resources are committed
8. Staff are aware and trained
9. A development life cycle is required
10. It is planned, managed, measureable and measured
11. It is reviewed and audited

## Risk Management

Risk management is the process of identification, analysis and acceptance or mitigation of uncertainty in investment decisions. Essentially, risk management occurs any time an investor or [fund manager](http://www.investopedia.com/terms/f/fundmanager.asp) analyzes and attempts to quantify the potential for losses in an investment and then takes the appropriate action (or inaction) given his [investment objectives](http://www.investopedia.com/terms/i/investmentobjective.asp) and [risk tolerance](http://www.investopedia.com/terms/r/risktolerance.asp).

## BREAKING DOWN 'Risk Management'

Inadequate risk management can result in severe consequences for companies as well as individuals. For example, the [recession](http://www.investopedia.com/terms/r/recession.asp) that began in 2008 was largely caused by the [loose credit](http://www.investopedia.com/terms/l/loose_credit.asp) risk management of financial firms.

Risk management occurs everywhere in the financial world. It occurs when an investor buys low-risk [government bonds](http://www.investopedia.com/terms/g/government-bond.asp) over more risky corporate debt, when a fund manager [hedges](http://www.investopedia.com/terms/h/hedge.asp) his currency exposure with currency [derivatives](http://www.investopedia.com/terms/d/derivative.asp) and when a bank performs a credit check on an individual before issuing a personal [line of credit](http://www.investopedia.com/terms/l/lineofcredit.asp).

## How Do Investors Measure Risk?

Investors use a variety of tactics to ascertain risk. In some cases, they look at the average return of an investment, and they find its average standard deviation over the same time period. Then, they apply a bell curve to that number, which dictates that the expected return of the investment is likely to be one standard deviation from the average two-thirds of the time and two standard deviations from the average deviation 95% of the time. This helps investors evaluate risk numerically. If they believe that they can tolerate the risk, financially and emotionally, they invest.

## What Is Enterprise Risk Management?

Enterprise risk management (ERM) encompasses all kinds of risks throughout an organization, and it creates plans for managing that risk. Industries such as aviation, construction, public health, international development, banking, finance and insurance utilize ERM. People who work with ERM focus on assessing the risks relevant to their companies or industries, prioritizing those risks, and making informed decisions to mitigate them.

## What Are Risk Management Plans?

Project managers create risk management plans to estimate the impact of various risks and outline possible responses if a certain risk materializes. For example, the Environmental Protection Agency (EPA) requires facilities that deal with extremely hazardous substances to develop risk management plans to address what they are doing to mitigate risks and what they will do if an accident occurs.

**Security Architecture And Design**

Security Architecture is one component of a products/systems overall architecture and is developed to provide guidance during the design of the product/system.

Security Architecture is the design artifacts that describe how the security controls (= security countermeasures) are positioned and how they relate to the overall systems architecture. These controls serve the purpose to maintain the system’s quality attributes such as confidentiality, integrity and availability. A security policy is a statement that outlines how entities access each other, what operations different entities can carry out, what level of protection is required for a system or software product, and what actions should be taken when these requirements are not me.

A security model outlines the requirements necessary to properly support and implement a certain security policy.

1. [Computer Systems Architecture](https://en.wikibooks.org/wiki/Security_Architecture_and_Design/Computer_Systems_Architecture)
2. [Systems Security Architecture](https://en.wikibooks.org/wiki/Security_Architecture_and_Design/Systems_Security_Architecture)
3. [Security Models](https://en.wikibooks.org/wiki/Security_Architecture_and_Design/Security_Models)
4. [Security Product Evaluation Methods and Criteria](https://en.wikibooks.org/wiki/Security_Architecture_and_Design/Security_Product_Evaluation_Methods_and_Criteria)



It covers the following :

* **Formal architecture:**Conceptually understanding the structure and behavior of a complex entity is required before attempting to secure it. Architectures map a system's components, interactions and interdependencies in one cohesive model.
* **System architecture:**The structures of hardware and software components of common systems, and how security can be implemented.
* **Security models:** The symbolic representations of policy that map the objectives of the policy makers to a set of rules that software and systems must follow under various system conditions.
* **System evaluation, certification and accreditation:** Methods used to examine the security-relevant parts of a system (e.g., reference monitor,[access control](http://searchsecurity.techtarget.com/definition/access-control) and [kernel](http://searchenterpriselinux.techtarget.com/definition/kernel) protection mechanisms), and how certification and accreditation are confirmed.

### Formal architecture

### Formal architecture development was covered in the [Information Security Governance and Risk Management domain](http://searchsecurity.techtarget.com/feature/CISSP-Essentials-training-Domain-1-Security-Management-Practices) in the context of organizational security programs and enterprise security [frameworks](http://whatis.techtarget.com/definition/framework). In this domain, the same type of approach to architecture is explored but in the context of system architecture. An architecture is a tool used to conceptually understand the structure and behavior of a complex entity. An architecture description is a formal explanation and representation of a system, the components that make up the system, the interactions and interdependencies between those components, and the relationship to the environment.

**System design**

In the system design phase, system requirement specifications are gathered and modeling languages are used to establish how the system will accomplish design goals (e.g., required functionality, compatibility, fault tolerance, extensibility, security, usability and maintainability). The modeling language is commonly graphical to visualize the system from a static structural view and a dynamic behavioral view. This makes it easier to understand what the components within the system need to accomplish individually, as well as how they work together to accomplish larger, established architectural goals. In this phase, security models that help construct the design of the system to meet the architectural goals

### System architecture

### Computer architecture encompasses all the parts of a computer system that are necessary for it to function, including the [operating system](http://whatis.techtarget.com/definition/operating-system-OS), memory[chips](http://whatis.techtarget.com/definition/chip), logic circuits, storage devices, [input and output devices](http://whatis.techtarget.com/definition/input-output-I-O), security components, [buses](http://searchstorage.techtarget.com/definition/bus) and networking interfaces. The interrelationships and internal workings of all these parts can be quite complex; making them work together in a secure fashion requires complicated methods and mechanisms. The more you understand how these different pieces work and process data, the more you will understand how vulnerabilities actually occur and how countermeasures work to impede and hinder these threats from being introduced, found and exploited.

**Security models**

An important concept in the design and analysis of secure systems is the security model as it incorporates the security policy to be enforced in the system. A model is a symbolic representation of a policy; it maps the desires of the policymakers into a set of rules that a computer system must follow by specifying explicit data structures and techniques necessary to enforce the security policy. A security model is usually represented in mathematical and analytical ideas, which are then mapped to system specifications and developed by programmers through programming code.



**Security Issues In Hardware**

Physical security/hardware security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism. Physical security is often overlooked (and its importance underestimated) in favor of more technical and dramatic issues such as hacking, [virus](http://searchsecurity.techtarget.com/definition/virus)es, [Trojan](http://searchsecurity.techtarget.com/definition/Trojan-horse)s, and [spyware](http://searchsecurity.techtarget.com/definition/spyware). However, breaches of physical security can be carried out with little or no technical knowledge on the part of an attacker. Moreover, accidents and natural disasters are a part of everyday life, and in the long term, are inevitable.

There are three main components to physical security/hardware security. First, obstacles can be placed in the way of potential attackers and sites can be hardened against accidents and environmental disasters. Such measures can include multiple locks, fencing, walls, fireproof safes, and water sprinklers. Second, surveillance and notification systems can be put in place, such as lighting, heat sensors, smoke detectors, intrusion detectors, alarms, and cameras. Third, methods can be implemented to apprehend attackers (preferably before any damage has been done) and to recover quickly from accidents, fires, or natural disasters.

**Data Storage Device and Downloadable Devices**

**Data Storage Devices**

A data storage device is a device for [recording](https://en.wikipedia.org/wiki/Recording) (storing) [information](https://en.wikipedia.org/wiki/Information) (data). Recording can be done using virtually any form of [energy](https://en.wikipedia.org/wiki/Energy), spanning from manual muscle power in [handwriting](https://en.wikipedia.org/wiki/Handwriting), to acoustic vibrations in [phonographic](https://en.wikipedia.org/wiki/Phonograph) recording, to electromagnetic energy modulating [magnetic tape](https://en.wikipedia.org/wiki/Magnetic_tape) and [optical discs](https://en.wikipedia.org/wiki/Optical_disc).

A storage device may hold information, process information, or both. A device that only holds information is a recording [medium](https://en.wikipedia.org/wiki/Medium_%28communication%29). Devices that process information (data storage equipment) may either access a separate portable (removable) recording medium or a permanent component to store and retrieve data.

Electronic data storages require electrical power to store and retrieve that data. Most storage devices that do not require [vision](https://en.wikipedia.org/wiki/Visual_perception) and a brain to read data fall into this category. Electromagnetic data may be stored in either an analog [data](https://en.wikipedia.org/wiki/Data) or [digital data](https://en.wikipedia.org/wiki/Digital_data) format on a variety of media. This type of data is considered to be [electronically encoded](https://en.wikipedia.org/wiki/Machine-readable_medium) data, whether it is electronically stored in a [semiconductor](https://en.wikipedia.org/wiki/Semiconductor) [device](https://en.wikipedia.org/wiki/Computer_data_storage), for it is certain that a semiconductor device was used to record it on its medium. Most electronically processed data storage media (including some forms of [computer data storage](https://en.wikipedia.org/wiki/Computer_data_storage)) are considered permanent (non-volatile) storage, that is, the data will remain stored when power is removed from the device. In contrast, most electronically stored information within most types of semiconductor (computer chips) [microcircuits](https://en.wikipedia.org/wiki/Microcircuit) are [volatile memory](https://en.wikipedia.org/wiki/Volatile_memory), for it vanishes if power is removed.

Except for [barcodes](https://en.wikipedia.org/wiki/Barcode), [OCR](https://en.wikipedia.org/wiki/Optical_character_recognition), and [MICR](https://en.wikipedia.org/wiki/Magnetic_ink_character_recognition) data, electronic data storage is easier to revise and may be more cost effective than alternative methods due to smaller physical space requirements and the ease of replacing (rewriting) data on the same medium. However, the durability of methods such as printed data is still superior to that of most electronic storage media. The durability limitations may be overcome with the ease of duplicating ([backing-up](https://en.wikipedia.org/wiki/Backup)) electronic data.

**Downloadable Devices**

Peripheral devices are traditionally considered to be secured, and therefore, these devices can be vulnerable to security attacks. This include:

* Universal Serial Bus (USB) drives
* USB patch cords that can be connected to a computer system using mini connectors or micro connectors.
* Electronic notebooks that are similar to laptops but are limited in application.
* Personal Digital Assistants (PDAs)

The issue with most of the downloadable devices is the threat that an external, unseen entity can create. You cannot easily detect threats to these devices. Therefore, they could be more vulnerable to security attacks in comparison with other devices/systems.

Some of the threats to downloadable devices are

#### Application-Based Threats

Downloadable applications can present many types of security issues for mobile devices. “Malicious apps” may look fine on a download site, but they are specifically designed to commit fraud. Even some legitimate software can be exploited for fraudulent purposes.

* **Malware** is software that performs malicious actions while installed on your phone. Without your knowledge, malware can make charges to your phone bill, send unsolicited messages to your contact list, or give an attacker control over your device.
* **Spyware** is designed to collect or use private data without your knowledge or approval. Data commonly targeted by spyware includes phone call history, text messages, user location, browser history, contact list, email, and private photos. This stolen information could be used for identity theft or financial fraud.

#### Web-based Threats

Because mobile devices are constantly connected to the Internet and frequently used to access web-based services, web-based threats pose persistent issues for mobile devices:

* **Phishing Scams** use email, text messages, Facebook, and Twitter to send you links to websites that are designed to trick you into providing information like passwords or account numbers. Often these messages and sites are very different to distinguish from those of your bank or other legitimate sources.
* **Drive-By Downloads** can automatically download an application when you visit a web page. In some cases, you must take action to open the downloaded application, while in other cases the application can start automatically.

#### Network Threats

Mobile devices typically support cellular networks as well as local wireless networks (WiFi, Bluetooth). Both of these types of networks can host different classes of threats:

* **Network exploits** take advantage of flaws in the mobile operating system or other software that operates on local or cellular networks. Once connected, they can install malware on your phone without your knowledge.
* **Wi-Fi Sniffing** intercepts data as it is traveling through the air between the device and the WiFi access point. Many applications and web pages do not use proper security measures, sending unencrypted data across the network that can be easily read by someone who is grabbing data as it travels.

#### Physical Threats

Mobile devices are small, valuable and we carry them everywhere with us, so their physical security is also an important consideration. Lost or Stolen Devices are one of the most prevalent mobile threats. The mobile device is valuable not only because the hardware itself can be re-sold on the black market, but more importantly because of the sensitive personal and organization information it may contain.

**Physical Security Of Information Assets**

Without paying proper attention to the physical security of information asset your IT assets and infrastructure are always under security threats from known or  unknown sources or from accidental hazards. An IT security manager or designer will always need to pay equal or even more attention to ensure that his all the information assets are physically secured. It is not necessary that all the physical security risk to IT assets can be only from physical break into the IT server or assets room, but there are major risk related to environmental risks such as fire. To control the physical security of all IT assets you need to identify all the assets that you consider sensitive and important for your organization. The physical security of IT assets can be broadly categorized based on the following criteria:

* Security of Asset Location
* Human access control to the security room
* Environmental control

**Security of asset location**

The location of the information asset room need to physical secured. It is always a good practice not to disclose the location of your server room to public. The lesser people know about the location of your server room the better. First of all, you need to make sure that there one entry to your server room including one emergency exit door. Secondly, the entrance of the access door should not be directly visible to the location of your office where the majority of the officials work. Thirdly, before the main access door there should be another small door or space to reduce the risk of piggy backing.

**Human access control**

Before entering the server room all the personal need to be authorized to enter the room-there can be an exception to the daily maintenance team. But it is better to have the presence of a supervisor when maintence works are carried out. All the personals need to be physically verified and must carry an identity card, if possible implement digital access control or any biometric access control. The security person before the access room must be present always and they there may be a pool of security guards who will be only duty so as they can be familiar with the faces entering the room on regular basis. Finally, there should be close circuit camera both in and outside of the asset room and you need to make sure the access to the digital recording devices are properly monitored and log.

**Environmental security control**

You need to make sure that all the equipment installed inside the server rooms are being auditor regularly. Make sure there are at least two emergency power-off switches for the server room itself-one inside and the other outside the room. All the electrical wiring should be placed inside fire-resistance panels and if there are any office desk or cabinets, then use only those equipments made of fire-resistance materials. Any kind of food intake must be strictly prohibited in the server room.

**CCTV**

Closed-circuit television (CCTV), also known as video surveillance, is the use of [video cameras](https://en.wikipedia.org/wiki/Video_camera) to transmit a signal to a specific place, on a limited set of monitors. It differs from [broadcast television](https://en.wikipedia.org/wiki/Broadcast_television) in that the signal is not openly transmitted, though it may employ point to point (P2P), point to multipoint (P2MP), or mesh wireless links. Though almost all video cameras fit this definition, the term is most often applied to those used for [surveillance](https://en.wikipedia.org/wiki/Surveillance) in areas that may need monitoring such as banks, casinos, airports, military installations, and convenience stores. [Video telephony](https://en.wikipedia.org/wiki/Videotelephony) is seldom called "CCTV" but the use of video in [distance education](https://en.wikipedia.org/wiki/Distance_education), where it is an important tool, is often so called.

In industrial plants, CCTV equipment may be used to observe parts of a process from a central control room, for example when the environment is not suitable for humans. CCTV systems may operate continuously or only as required to monitor a particular event. A more advanced form of CCTV, utilizing [digital video recorders](https://en.wikipedia.org/wiki/Digital_video_recorder), (DVRs), provides recording for possibly many years, with a variety of quality and performance options and extra features (such as [motion detection](https://en.wikipedia.org/wiki/Motion_detection) and email alerts). More recently, decentralized [IP cameras](https://en.wikipedia.org/wiki/IP_camera), some equipped with megapixel sensors, support recording directly to [network-attached storage](https://en.wikipedia.org/wiki/Network-attached_storage) devices, or internal flash for completely stand-alone operation. Surveillance of the public using CCTV is particularly common in many areas around the world. In recent years, the use of [body worn video](https://en.wikipedia.org/wiki/Body_worn_video) cameras has been introduced as a new form of surveillance.

**Backup Security Measures**

Data backups are an essential element of good storage security, but they're often the source of security woes. In fact, a significant percentage of security breaches can be attributed to the mismanagement and mishandling of data backups. Many storage professionals responsible for backups believe that the mere existence of a process for replicating sensitive data is all that's needed to keep the organization secure. But that's only half the battle. It's what can be done with the data backups *after* the fact that introduces an entirely different set of risks that are often overlooked. Here are 10 ways you can ensure that your data backups are secure:

1. Ensure your security policies include backup-related systems within their scope. Practically every type of security policy -- from access controls to physical security to system monitoring -- applies directly to data backups.
2. Include your data backup systems in your [disaster recovery](http://searchdisasterrecovery.techtarget.com/) and incident response plans. Data backups can be breached, compromised or destroyed. Be it a malware outbreak, employee break-in or hurricane -- otherwise good backups can be adversely affected and you need to have a plan outlining what you're going to do if that time comes.
3. Assign backup software access rights only to those who have a business need to be involved in the backup process. Be sure not to overlook any Web-based interfaces that provide backup access and keep your original backup software media secured as well.
4. Store your backups offsite or at least in another building. I know this sounds pretty basic, but I still see it a lot. A fire or other incident could be all that's needed to take out your data center *and* your backups in one fell swoop.
5. However you choose to store your backups -- be it on tape, network-attached storage (NAS), or external drives -- be sure to control access to the room/car/house in which the backups stored. Handle your backup media as you would any other critical hardware.
6. Use a fireproof *and* media-rated safe. Many people store their backups in a "fireproof" safe, but typically one that's only rated for paper storage. Backup media such as tapes, optical disks and magnetic drives have a lower burning/melting point than paper and a standard fireproof safe only serves to provide a false sense of security.
7. Find out the security measures that your vendors for offsite storage, data center and courier services are taking to ensure that your backups remain safe in their hands. Although lawyers like good contracts, they're not enough. Contracts do offer fallback measures but they won't keep sensitive data from being exposed in the first place, so make sure reasonable and consistent security measures are taking place with any vendor that has a hand in your backups.
8. Password-protect your backups at a minimum. Passwords aren't foolproof because some people with special skills and tools may be able to crack the code, but it is a level of security that should be considered. That said, password-protection is better than nothing, and at least provides a layer of security.
9. [Encrypt](http://searchdatabackup.techtarget.com/tip/Where-should-you-encrypt-your-data) your backups if your software and hardware support it. As with laptop computers and other mobile devices, portable backup media need to be encrypted with strong passphrases especially if they're ever removed from the premises. Encryption implemented and managed in the right way serves as an excellent last layer of defense. It also helps provide peace of mind knowing that the worst outcome is that you'll have to buy new backup media -- especially when it comes to compliance and data breach notifications.
10. You've heard it a thousand times but it deserves repeating: Your backups are only as good as what's on the backup media. There are two sides to this coin. First, make sure your backing up everything that's important. Most backups are server-centric but what about all of that unstructured data scattered about on your workstations and mobile devices that isn't getting backed up? Second, test your backups occasionally -- especially if you're using tape. There's nothing worse than recovering from a loss and only to find out you backed up the wrong data or no data at all.

**NOTE:**  **For “Access Control, Intrusion Detection System & types of Backup Recovery” kindly refer notes of UNIT-2.**