**Unit-I**

**What is Information Security?**

**Information Security** is not only about securing information from unauthorized access. Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be physical or electronic one. Information can be anything like Your details or we can say your profile on social media, your data in mobile phone, your biometrics etc. Thus Information Security spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media etc.

During First World War, Multi-tier Classification System was developed keeping in mind sensitivity of information. With the beginning of Second World War formal alignment of Classification System was done. Alan Turing was the one who successfully decrypted Enigma Machine which was used by Germans to encrypt warfare data.

Information Security programs are build around 3 objectives, commonly known as CIA – Confidentiality, Integrity, Availability.

1. **Confidentiality –** means information is not disclosed to unauthorized individuals, entities and process. For example if we say I have a password for my Gmail account but someone saw while I was doing a login into Gmail account. In that case my password has been compromised and Confidentiality has been breached.
2. **Integrity –** means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way. For example if an employee leaves an organisation then in that case data for that employee in all departments like accounts, should be updated to reflect status to JOB LEFT so that data is complete and accurate and in addition to this only authorized person should be allowed to edit employee data.
3. **Availability –** means information must be available when needed. For example if one needs to access information of a particular employee to check whether employee has outstanded the number of leaves, in that case it requires collaboration from different organizational teams like network operations, development operations, incident response and policy/change management.
Denial of service attack is one of the factor that can hamper the availability of information.

# Evolution of Information Security

In the same way that computers and the use of the internet has exponentially increased over the last few decades, so has information security. Simply trying to stay up to date on social media and internet based threats is a job of its own. Funding, the level of security and amount of time spent regarding information security has steadily increased over the years, and will continue to rise in the near future. Many companies have struggled to evolve and stay up to date with information security trends. If your company falls in this boat, consider partnering with TrustMAPP, an information security platform designed to help you gain confidence and maintain advanced cyber security, no matter what the future has in store.

### How Information Security Has Changed

* **The 1990’s** – Known as “IT Security” at this time, a security focus was placed on overseeing protective software such as antivirus and firewalls. Most companies invested in external security blankets that they could point to for guidance if a security breach occurred. Not many information security projects occurred during this time because it was unknown on how to comply with regulations. Lastly, few dollars were allocated for funding information security requests during the 1990’s.
* **The 2000’s** – New technology such as signature based communication made personal information better protected. New concerns regarding hacking and the growth of the world wide web placed a strong emphasis on protection from security breaches. Funding consistently increased when it came to information security needs. The Software Development Life Cycle created security guidelines and standards designed to reduce vulnerabilities across companies. From seeing the harm that security breaches can do to a firm, many executives began to fund advanced information security so that the brand itself did not get damaged and so that the firm did not become the next big name on the news for experiencing a data breach.
* **The Future** – With the new cloud based concept, companies are having to find new ways to oversee and protect their valuable information. Nowadays, information security is a key driver in corporate strategy across a firm. Security doesn’t stop at computers any longer. Now, cell phones, tablets and at home computers must be analyzed and protected from any potential security threats as well. Case in point, information security is an ever evolving topic that should be a high priority within your firm

## **IT Security Audit**

A cyber security audit consists of five steps:

1. Define the objectives.
2. Plan the audit.
3. Perform the auditing work.
4. Report the results.
5. Take necessary action.

### 1. Define the Objectives

Lay out the goals that the auditing team aims to achieve by conducting the IT security audit. Make sure to clarify the business value of each objective so that specific goals of the audit align with the larger goals of your company.

Use this list of questions as a starting point for brainstorming and refining your own list of objectives for the audit.

* Which systems and services do you want to test and evaluate?
* Do you want to audit your digital IT infrastructure, your physical equipment and facilities, or both?
* Is disaster recovery on your list of concerns? What specific risks are involved?
* Does the audit need to be geared towards proving compliance with a particular regulation?

### 2. Plan the Audit

A thoughtful and well-organized plan is crucial to success in an IT security audit.

You’ll want to define the roles and responsibilities of the management team and the IT system administrators assigned to perform the auditing tasks, as well as the schedule and methodology for the process. Identify any monitoring, reporting and [data classification](https://blog.netwrix.com/2020/09/02/data-classification/) tools that the team will use and any logistical issues they may face, like taking equipment offline for evaluation.

Once you’ve decided on all the details, document and circulate the plan to ensure that all staff members have a common understanding of the process before the audit begins.

### 3. Perform the Auditing Work

The auditing team should conduct the audit according to the plan and methodologies agreed upon during the planning phase. This will typically include running scans on IT resources like file-sharing services, database servers and SaaS applications like Office 365 to assess [network security](https://blog.netwrix.com/2019/07/09/10-fundamental-elements-of-network-security-to-improve-data-security/), data access levels, [user access rights](https://www.netwrix.com/how_to_get_ad_user_permissions_report.html?itm_source=blog&itm_medium=context&itm_campaign=it-security-audit&itm_content=none&cID=70170000000kgEZ) and other system configurations. It’s also a good idea to physically inspect the data center for resilience to fires, floods and power surges as part of a disaster recovery evaluation.

During this process, interview employees outside the IT team to assess their knowledge of security concerns and adherence to company [security policy](https://blog.netwrix.com/2021/02/25/security-policy/), so any holes in your company’s security procedures can be addressed moving forward.

Be sure to document all findings uncovered during the audit.

### 4. Report the Results

Compile all your audit-related documentation into a formal report that can be given to management stakeholders or the regulatory agency. The report should include a list of any security risks and vulnerabilities detected in your systems, as well as actions that IT staff recommend taking to mitigate them.

### 5. Take Necessary Action

Finally, follow through with the recommendations outlined in your audit report. Examples of security-enhancement actions can include:

* Performing remediation procedures to fix a specific security flaw or weak spot.
* Training employees in [data security compliance](https://blog.netwrix.com/2019/08/06/data-security-compliance-essentials-only/) and security awareness.
* Adopting additional best practices for handling sensitive data and recognizing signs of malware and phishing attacks.
* Acquiring new technologies to harden existing systems and regularly monitor your infrastructure for security risk

# What is risk analysis?

Risk analysis is the process of identifying and analyzing potential issues that could negatively impact key business initiatives or projects. This process is done in order to help organizations avoid or [mitigate those risks](https://www.techtarget.com/searchdisasterrecovery/definition/risk-mitigation).

Performing a risk analysis includes considering the possibility of adverse events caused by either natural processes, like severe storms, earthquakes or floods, or adverse events caused by malicious or inadvertent human activities. An important part of risk analysis is identifying the potential for harm from these events, as well as the likelihood that they will occur.

## Why is risk analysis important?

Enterprises and other organizations use risk analysis to:

* anticipate and reduce the effect of harmful results from adverse events;
* evaluate whether the potential risks of a project are balanced by its benefits to aid in the decision process when evaluating whether to move forward with the project;
* plan responses for technology or equipment failure or loss from adverse events, both natural and human-caused; and
* identify the impact of and prepare for changes in the enterprise environment, including the likelihood of new competitors entering the market or changes to government regulatory policy.

## What are the benefits of risk analysis?

Organizations must understand the risks associated with the use of their information systems to effectively and efficiently protect their information assets.

Risk analysis can help an organization improve its security in a number of ways. Depending on the type and extent of the risk analysis, organizations can use the results to help:

**THIS ARTICLE IS PART OF**

* identify, rate and compare the overall impact of risks to the organization, in terms of both financial and organizational impacts;
* identify [gaps in security and determine the next steps](https://www.techtarget.com/searchsecurity/tip/How-to-perform-a-cybersecurity-risk-assessment-step-by-step) to eliminate the weaknesses and strengthen security;
* enhance communication and decision-making processes as they relate to information security;
* improve [security policies and procedures](https://www.techtarget.com/searchsecurity/The-ultimate-guide-to-cybersecurity-planning-for-businesses) and develop cost-effective methods for implementing these information security policies and procedures;
* put security controls in place to [mitigate the most important risks](https://www.techtarget.com/searchcio/feature/7-risk-mitigation-strategies-to-protect-business-operations);
* increase employee awareness about security measures and risks by highlighting best practices during the risk analysis process; and
* understand the financial impacts of potential security risks.

Done well, risk analysis is an important tool for managing costs associated with risks, as well as for aiding an organization's decision-making process.

## Steps in risk analysis process

The risk analysis process usually follows these basic steps:

1. **Conduct a**[**risk assessment**](https://searchcompliance.techtarget.com/definition/risk-assessment)**survey:** This first step, getting input from management and department heads, is critical to the risk assessment process. The risk assessment survey is a way to begin documenting specific risks or threats within each department.
2. **Identify the risks:** The reason for performing risk assessment is to evaluate an IT system or other aspect of the organization and then ask: What are the risks to the software, hardware, data and IT employees? What are the possible adverse events that could occur, such as human error, fire, flooding or earthquakes? What is the potential that the integrity of the system will be compromised or that it won't be available?
3. **Analyze the risks:** Once the risks are identified, the risk analysis process should determine the likelihood that each risk will occur, as well as the [consequences linked to each risk](https://www.techtarget.com/searchcio/feature/4-basic-types-of-business-risks-in-the-enterprise) and how they might affect the objectives of a project.
4. **Develop a**[**risk management**](https://searchcompliance.techtarget.com/definition/risk-management)**plan:** Based on an analysis of which assets are valuable and which threats will probably affect those assets negatively, the risk analysis should produce control recommendations that can be used to mitigate, transfer, accept or avoid the risk.
5. **Implement the risk management plan:** The ultimate goal of risk assessment is to implement measures to remove or reduce the risks. Starting with the highest-priority risk, resolve or at least mitigate each risk so it's no longer a threat.
6. **Monitor the risks:** The ongoing process of identifying, treating and managing risks should be an important part of any risk analysis process.

The focus of the analysis, as well as the format of the results, will vary depending on the type of risk analysis being carried out.

**Security methodology**

Some protection methods are used to reduce security issues.

1. [**Authentication**](https://www.geeksforgeeks.org/difference-between-authentication-and-authorization/)**:**
Authentication is the process of recognizing or identifying a user’s identity whether it is true, real, or not. It’s simply a verification of claim whether you are who you say you are or not. There are many authentication methods available nowadays like password authentication that includes using a password, physical authentication that includes the scannable card or smart card or digital certificate, biometric authentication that includes signatures and fingerprints, or visual identification, and many more.
2. **Authorization :**
Authorization means to ensure whether you have permission to access on network or not. It’s simply a verification of permission either user has access or not. Some authorization methods are ACLs (Access Control Lists), Secure objects and methods, Access control for URL’s, etc.
3. [**Biometric System**](https://www.geeksforgeeks.org/what-is-biometrics/)**:**
A Biometric system is one of the most secure systems as it provides high security to the computer network. This system verifies the user’s identity based on some important characteristics that are physiological and behavioral features. Physiological features include face, eyes, fingerprints, hand. Behavioral features include voice, signature, etc.
4. [**Firewall**](https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/)**:**
A firewall is a method of network security that prevents the computer network from users that are not authorized to have access to a network. Firewalls can either be hardware or software or both. It acts as a barrier between unauthorized Internet users and private computer networks connected to the Internet. It blocks the message, viruses, hackers if they do not have authorized access and do not meet the security criteria as per requirement. Any message entering or leaving private computer networks connected to the Internet especially Intranet pass through the firewall. Firewall then checks each message and block if found unauthorized.

**How to build a security program**

There are six steps to implement this type of strategy:

* Identify your assets and related threats
* Identify and prioritize risks
* Implement foundational information security controls
* Build a robust information security program
* Develop a security improvement roadmap
* Establish executive support and organizational engagement around the program

Once you implement these steps, they could help keep risk at an acceptable level, so key stakeholders can respond quickly and appropriately to future threats.

#### **Identify Assets and Related Threats**

First, take stock of the data you have, then assess its value and threats that may impact it.

The elements necessary to begin building an effective risk-based program include knowing all about your data, including:

* Type
* Location
* Value
* Access rights
* Purpose
* Threats likely to materialize

A surprising number of organizations don’t know exactly where all their sensitive data resides.

For example, if your organization uses a third-party vendor as part of its IT ecosystem, and most organizations do, your data could be replicated and backed up in multiple places unknown to you.

#### **Identify and Prioritize Risks**

Identifying risk encompasses an examination of the people, processes, and systems with which your organization interacts.

Consider the possible objectives of an advanced persistent threat, a formidable threat actor, available attack vectors, and resources available for preventing a security breach. It’s also helpful to look ahead at emerging threats.

#### **Implement Foundational Information Security Controls**

After you identify risks, you can implement the foundational security controls and processes mentioned above. These should be operational and tested on a regular basis regardless of business size or complexity.

Your testing schedule will depend on several factors including your business model, information architecture, and risk exposure.

#### **Build a Robust Information Security Program**

Consider the following areas:

* **Governance and management**. Create organizational structure, processes, and leadership to define, manage, measure, and keep risk within tolerable levels.
* **Threat management**. Understand your adversaries and their tactics, techniques, and procedures to put appropriate protections in place and to help anticipate future threats.
* **Security monitoring and analysis**. Detect threats with even a basic security log to monitor your system and perform analysis on its output. The quick discovery of an intruder could be the difference between a security incident versus a full-scale breach.
* **Incident response**. Perform a mock incident event on an annual basis to test the program design. It’s important to have a defined process, engaged stakeholders, and native security logs available.
* **Data security**. Protect against unauthorized access to sensitive data by making sure inhouse tools like firewalls and security information and event management (SIEM) technology are installed and configured correctly.
* **Infrastructure security**. Choose adequate systems designed to protect an internet-connected business.

In addition to these core components, consider and implement input from internal audit, legal, and assurance departments so regulatory requirements and compliance standards are met.

#### **Develop a Security Improvement Roadmap**

Use your risk prioritization scorecard and chart to select the top risks to be reduce first. Typically, you can find these in the upper right quadrant of the risk prioritization chart.

This could involve process changes, incorporating new or updated technology into the organization, or additional staffing. These remediation efforts become the basis for new roadmap projects.

Costs, timelines, and staffing needs are identified for each project, along with estimated risk reduction values. Depending on the information security maturity of the business, the projects can be foundational, advanced, administrative, or technical in nature.

#### **Establish Executive Support and Organizational Engagement**

It’s the responsibility of information security leadership to clearly articulate the value of funding these programs and their potential to executive leadership.

One of leadership’s most important tasks is to secure appropriate funding and resources, which can be a daunting obstacle, especially if there’s a trend within the organization towards a higher-than-average risk tolerance.

However, information security should be an active board room topic. If it’s not, find a supporter or executive sponsor for the information security program. Inform this sponsor about information security, what the program aims to achieve, and expectations for the executive leaders so they can support security initiatives.

Quantifying risk in terms of dollars spent versus dollars lost is an effective way to get the attention and support of executive leadership.

Strategy and Tactics

To design and implement a secure cyberspace, some stringent strategies have been put in place. This chapter explains the major strategies employed to ensure cybersecurity, which include the following −

* Creating a Secure Cyber Ecosystem
* Creating an Assurance Framework
* Encouraging Open Standards
* Strengthening the Regulatory Framework
* Creating Mechanisms for IT Security
* Securing E-governance Services
* Protecting Critical Information Infrastructure

## **Strategy 1 − Creating a Secure Cyber Ecosystem**

The cyber ecosystem involves a wide range of varied entities like devices (communication technologies and computers), individuals, governments, private organizations, etc., which interact with each other for numerous reasons.

This strategy explores the idea of having a strong and robust cyber-ecosystem where the cyber-devices can work with each other in the future to prevent cyber-attacks, reduce their effectiveness, or find solutions to recover from a cyber-attack.

Such a cyber-ecosystem would have the ability built into its cyber devices to permit secured ways of action to be organized within and among groups of devices. This cyber-ecosystem can be supervised by present monitoring techniques where software products are used to detect and report security weaknesses.

A strong cyber-ecosystem has three symbiotic structures − **Automation, Interoperability,** and **Authentication**.

## **Strategy 2 − Creating an Assurance Framework**

The objective of this strategy is to design an outline in compliance with the global security standards through traditional products, processes, people, and technology.

To cater to the national security requirements, a national framework known as the **Cybersecurity Assurance Framework** was developed. It accommodates critical infrastructure organizations and the governments through "Enabling and Endorsing" actions.

**Enabling** actions are performed by government entities that are autonomous bodies free from commercial interests. The publication of "National Security Policy Compliance Requirements" and IT security guidelines and documents to enable IT security implementation and compliance are done by these authorities.

**Endorsing** actions are involved in profitable services after meeting the obligatory qualification standards

## **Strategy 3 − Encouraging Open Standards**

Standards play a significant role in defining how we approach information security related issues across geographical regions and societies. Open standards are encouraged to −

* Enhance the efficiency of key processes,
* Enable systems incorporations,
* Provide a medium for users to measure new products or services,
* Organize the approach to arrange new technologies or business models,
* Interpret complex environments, and
* Endorse economic growth.

## **Strategy 4 − Strengthening the Regulatory Framework**

The objective of this strategy is to create a secure cyberspace ecosystem and strengthen the regulatory framework. A 24X7 mechanism has been envisioned to deal with cyber threats through National Critical Information Infrastructure Protection Centre (NCIIPC). The Computer Emergency Response Team (CERT-In) has been designated to act as a nodal agency for crisis management.

Some highlights of this strategy are as follows −

* Promotion of research and development in cybersecurity.
* Developing human resource through education and training programs.
* Encouraging all organizations, whether public or private, to designate a person to serve as Chief Information Security Officer (CISO) who will be responsible for cybersecurity initiatives.
* Indian Armed Forces are in the process of establishing a cyber-command as a part of strengthening the cybersecurity of defense network and installations.
* Effective implementation of public-private partnership is in pipeline that will go a long way in creating solutions to the ever-changing threat landscape.

## **Strategy 5 − Creating Mechanisms for IT Security**

Some basic mechanisms that are in place for ensuring IT security are − link-oriented security measures, end-to-end security measures, association-oriented measures, and data encryption. These methods differ in their internal application features and also in the attributes of the security they provide. Let us discuss them in brief.

### **Link-Oriented Measures**

It delivers security while transferring data between two nodes, irrespective of the eventual source and destination of the data.

### **End-to-End Measures**

It is a medium for transporting Protocol Data Units (PDUs) in a protected manner from source to destination in such a way that disruption of any of their communication links does not violate security.

### **Association-Oriented Measures**

Association-oriented measures are a modified set of end-to-end measures that protect every association individually.

### **Data Encryption**

It defines some general features of conventional ciphers and the recently developed class of public-key ciphers. It encodes information in a way that only the authorized personnel can decrypt them.

## **Strategy 6 − Securing E-Governance Services**

Electronic governance (e-governance) is the most treasured instrument with the government to provide public services in an accountable manner. Unfortunately, in the current scenario, there is no devoted legal structure for e-governance in India.

Similarly, there is no law for obligatory e-delivery of public services in India. And nothing is more hazardous and troublesome than executing e-governance projects without sufficient cybersecurity. Hence, securing the e-governance services has become a crucial task, especially when the nation is making daily transactions through cards.

Fortunately, the Reserve Bank of India has implemented security and risk mitigation measures for card transactions in India enforceable from 1st October, 2013. It has put the responsibility of ensuring secured card transactions upon banks rather than on customers.

"E-government" or electronic government refers to the use of Information and Communication Technologies (ICTs) by government bodies for the following −

* Efficient delivery of public services
* Refining internal efficiency
* Easy information exchange among citizens, organizations, and government bodies
* Re-structuring of administrative processes.

## **Strategy 7 − Protecting Critical Information Infrastructure**

Critical information infrastructure is the backbone of a country’s national and economic security. It includes power plants, highways, bridges, chemical plants, networks, as well as the buildings where millions of people work every day. These can be secured with stringent collaboration plans and disciplined implementations.

Safeguarding critical infrastructure against developing cyber-threats needs a structured approach. It is required that the government aggressively collaborates with public and private sectors on a regular basis to prevent, respond to, and coordinate mitigation efforts against attempted disruptions and adverse impacts to the nation’s critical infrastructure.

Risk Analysis

What is risk analysis in information security?

[Information Security](https://www.tutorialspoint.com/questions/category/information-security)[Safe & Security](https://www.tutorialspoint.com/questions/category/safe-and-security)[Data Structure](https://www.tutorialspoint.com/questions/category/Data-Structure)

Risk analysis defines the review of risks related to the specific action or event. The risk analysis is used to information technology, projects, security issues and some other event where risks can be analysed based on a quantitative and qualitative basis.

There are some steps followed by a risk analysis process are as follows −

* **Establish the Risk Assessment Team** − The risk assessment team will be answerable for the collection, analysis, and documenting of the assessment results to management. It is essential that some aspects of the activity work flow be defined on the team, such as human resources, administrative processes, automated systems, and physical security.
* **Set the scope of the Project** − The assessment team should recognize at the outset the goals of the assessment project, department, or functional events to be assessed, the responsibilities of the members of the team, the personnel to be interviewed, the standards to be used, documentation to be inspected and operations to be checked.
* **Identify assets covered by the Assessment** − Assets can involve, but are not defined to, personnel, hardware, software, data (such as classification of sensitivity and criticality), facilities and current controls that security those assets. It is the key to recognize all assets related to the assessment project determined in the scope.
* **Categorize Potential Losses** − It can identify the losses that can result from some type of damage to an asset. Losses can result from physical damage, denial of service, alteration, unauthorized access or disclosure. Losses can be intangible, including the loss of the organizations’ credibility.
* **Identify Threats and Vulnerabilities** − A threat is an event, procedures, activity, or process that exploits a vulnerability to attack an asset. It involves natural threats, accidental threats, human accidental threats, and human malicious threats. These can involve power failure, biological contamination or hazardous chemical spills, acts of features, or hardware/software failure, data elimination or loss of integrity, sabotage, or theft or vandalism.

Vulnerability is a weakness which a threat will exploit to attack the assets. Vulnerabilities can be recognized by addressing the following in the data collection process such as physical security, environment, system security, communications security, personnel security, plans, policies, processes, management, support, etc.

* **Identify existing Controls** − Controls are safeguards that decrease the probability that a threat will exploit a vulnerability to strongly attack an asset. It can recognize those safeguards that are currently executed, and determine their effectiveness in the context of the current analysis.
* **Analyze the Data** − In this step, all the collected data will be used to decide the actual risks to the assets under consideration. A method to analyze data contains preparing a record of assets and displaying corresponding threats, type of loss and vulnerability. Analysis of this data should contains an assessment of the possible frequency of the potential fall

**Threats to Information Security**

* Difficulty Level : [Medium](https://www.geeksforgeeks.org/medium/)
* Last Updated : 28 Jun, 2022

Information Security threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.

**Threat** can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest.

**Software attacks** means attack by Viruses, Worms, Trojan Horses etc. Many users believe that malware, virus, worms, bots are all same things. But they are not same, only similarity is that they all are malicious software that behaves differently.

**Malware** is a combination of 2 terms- Malicious and Software. So Malware basically means malicious software that can be an intrusive program code or anything that is designed to perform malicious operations on system. Malware can be divided in 2 categories:

1. Infection Methods
2. Malware Actions

Malware on the **basis of Infection** Method are following:

1. **Virus –** They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc and then they travel all over the Internet. The Creeper Virus was first detected on ARPANET. Examples include File Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.
2. **Worms –** Worms are also self-replicating in nature but they don’t hook themselves to the program on host computer. Biggest difference between virus and worms is that worms are network-aware. They can easily travel from one computer to another if network is available and on the target machine they will not do much harm, they will, for example, consume hard disk space thus slowing down the computer.
3. **Trojan –** The Concept of Trojan is completely different from the viruses and worms. The name Trojan is derived from the ‘Trojan Horse’ tale in Greek mythology, which explains how the Greeks were able to enter the fortified city of Troy by hiding their soldiers in a big wooden horse given to the Trojans as a gift. The Trojans were very fond of horses and trusted the gift blindly. In the night, the soldiers emerged and attacked the city from the inside.

Their purpose is to conceal themselves inside the software that seem legitimate and when that software is executed they will do their task of either stealing information or any other purpose for which they are designed.

They often provide backdoor gateway for malicious programs or malevolent users to enter your system and steal your valuable data without your knowledge and permission. Examples include FTP Trojans, Proxy Trojans, Remote Access Trojans etc.

1. **Bots –**: can be seen as advanced form of worms. They are automated processes that are designed to interact over the internet without the need for human interaction. They can be good or bad. Malicious bot can infect one host and after infecting will create connection to the central server which will provide commands to all infected hosts attached to that network called **Botnet.**

Malware on the **basis of Actions:**

1. **Adware –** Adware is not exactly malicious but they do breach privacy of the users. They display ads on a computer’s desktop or inside individual programs. They come attached with free-to-use software, thus main source of revenue for such developers. They monitor your interests and display relevant ads. An attacker can embed malicious code inside the software and adware can monitor your system activities and can even compromise your machine.
2. **Spyware –** It is a program or we can say software that monitors your activities on computer and reveal collected information to an interested party. Spyware are generally dropped by Trojans, viruses or worms. Once dropped they install themselves and sits silently to avoid detection.

One of the most common example of spyware is KEYLOGGER. The basic job of keylogger is to record user keystrokes with timestamp. Thus capturing interesting information like username, passwords, credit card details etc.

1. **Ransomware –** It is type of malware that will either encrypt your files or will lock your computer making it inaccessible either partially or wholly. Then a screen will be displayed asking for money i.e. ransom in exchange.
2. **Scareware –** It masquerades as a tool to help fix your system but when the software is executed it will infect your system or completely destroy it. The software will display a message to frighten you and force to take some action like pay them to fix your system.
3. **Rootkits –** are designed to gain root access or we can say administrative privileges in the user system. Once gained the root access, the exploiter can do anything from stealing private files to private data.
4. **Zombies –** They work similar to Spyware. Infection mechanism is same but they don’t spy and steal information rather they wait for the command from hackers.

* **Theft of intellectual property** means violation of intellectual property rights like copyrights, patents etc.
* **Identity theft** means to act someone else to obtain person’s personal information or to access vital information they have like accessing the computer or social media account of a person by login into the account by using their login credentials.
* **Theft of equipment and information** is increasing these days due to the mobile nature of devices and increasing information capacity.
* **Sabotage** means destroying company’s website to cause loss of confidence on part of its customer.
* **Information extortion** means theft of company’s property or information to receive payment in exchange. For example ransomware may lock victims file making them inaccessible thus forcing victim to make payment in exchange. Only after payment victim’s files will be unlocked.

These are the old generation attacks that continue these days also with advancement every year. Apart from these there are many other threats. Below is the brief description of these new generation threats.

* **Technology with weak security –** With the advancement in technology, with every passing day a new gadget is being released in the market. But very few are fully secured and follows Information Security principles. Since the market is very competitive Security factor is compromised to make device more up to date. This leads to theft of data/ information from the devices
* **Social media attacks –** In this cyber criminals identify and infect a cluster of websites that persons of a particular organization visit, to steal information.
* **Mobile Malware –**There is a saying when there is a connectivity to Internet there will be danger to Security. Same goes for Mobile phones where gaming applications are designed to lure customer to download the game and unintentionally they will install malware or virus on the device.
* **Outdated Security Software –** With new threats emerging everyday, updation in security software is a prerequisite to have a fully secured environment.
* **Corporate data on personal devices –** These days every organization follows a rule BYOD. BYOD means Bring your own device like Laptops, Tablets to the workplace. Clearly BYOD pose a serious threat to security of data but due to productivity issues organizations are arguing to adopt this.
* **Social Engineering –** is the art of manipulating people so that they give up their confidential information like bank account details, password etc. These criminals can trick you into giving your private and confidential information or they will gain your trust to get access to your computer to install a malicious software- that will give them control of your computer. For example email or message from your friend, that was probably not sent by your friend. Criminal can access your friends device and then by accessing the contact list, he can send infected email and message to all contacts. Since the message/ email is from a known person recipient will definitely check the link or attachment in the message, thus unintentionally infecting the computer.

# Active and Passive attacks in Information Security

* **Difficulty Level :** [Medium](https://www.geeksforgeeks.org/medium/)
* **Last Updated :** 24 Dec, 2021

**Active attacks:** An Active attack attempts to alter system resources or affect their operations. Active attacks involve some modification of the data stream or the creation of false statements. Types of active attacks are as follows:

* Masquerade
* Modification of messages
* Repudiation
* Replay
* Denial of Service

### **Masquerade –**

A masquerade attack takes place when one entity pretends to be a different entity. A Masquerade attack involves one of the other forms of active attacks.  If an authorization procedure isn’t always absolutely protected, it is able to grow to be extraordinarily liable to a masquerade assault. Masquerade assaults may be performed using the stolen passwords and logins, with the aid of using finding gaps in programs, or with the aid of using locating a manner across the authentication process.

### **Modification of messages –**

It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect. Modification is an attack on the integrity of the original data. It basically means that unauthorized parties not only gain access to data but also spoof the data by triggering denial-of-service attacks, such as altering transmitted data packets or flooding the network with fake data. Manufacturing is an attack on authentication. For example, a message meaning “Allow JOHN to read confidential file X” is modified as “Allow Smith to read confidential file X”.

### **Repudiation –**

This attack occurs when the network is not completely secured or the login control has been tampered with. With this attack, the author’s information can be changed by actions of a malicious user in order to save false data in log files, up to the general manipulation of data on behalf of others,  similar to the spoofing of e-mail messages.

### **Replay –**

It involves the passive capture of a message and its subsequent transmission to produce an authorized effect. In this attack, the basic aim of the attacker is to save a copy of the data originally present on that particular network and later on use this data for personal uses. Once the data is corrupted or leaked it is insecure and unsafe for the users.

### **Denial of Service –**

It prevents the normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network either by disabling the network or by overloading it with messages so as to degrade performance.

**Passive attacks:** A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring transmission. The goal of the opponent is to obtain information that is being transmitted. Types of Passive attacks are as follows:

* The release of message content
* Traffic analysis

### **The release of message content –**

Telephonic conversation, an electronic mail message, or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

### **Traffic analysis –**

Suppose that we had a way of masking (encryption) information, so that the attacker even if captured the message could not extract any information from the message.
The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.
The most useful protection against traffic analysis is encryption of SIP traffic. To do this, an attacker would have to access the SIP proxy (or its call log) to determine who made the call.

cyber threats

Types of cyber threats your institution should be aware of include:

* Malware
* Ransomware
* Distributed denial of service (DDoS) attacks
* Spam and Phishing
* Corporate Account Takeover (CATO)
* Automated Teller Machine (ATM) Cash Out

## Malware

Malware is also known as malicious code or malicious software. Malware is a program inserted into a system to compromise the confidentiality, integrity, or availability of data. It is done secretly and can affect your data, applications, or operating system. Malware has become one of the most significant external threat to systems. Malware can cause widespread damage and disruption, and requires huge efforts within most organizations.

Spyware, a malware intended to violate privacy, has also become a major concern to organizations. Although privacy-violating malware has been in use for many years, it has become much more common recently. Spyware invades many systems to track personal activities and conduct financial fraud.

Organizations also face similar threats from several forms of non-malware threats. These forms of cyber threats are often associated with malware. A more common form is phishing. Phishing involves tricking individuals into revealing sensitive or personal information.

**Tips for preventing Malware from the**[**National Institute of Standards and Technology (NIST) Guide to Malware Incident Prevention and Handling**](http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-83.pdf)**:**

* Require e-mail file attachments to be scanned and saved to local drives or removable media.
* Don’t allow certain types of files (e.g., .exe files) to be sent or received by e-mail.
* Restrict removable media, such as CDs or flash drives, on systems that are high risk.
* Limit the number of users with administrator-level access or privileges.
* Ensure systems are updated regularly with operating system and application upgrades and patches.

## Ransomware

Ransomware prevents or limits users from accessing their system via malware. Ransomware asks you to pay a ransom using online payment methods to regain access to your system or data. Online payment methods usually include virtual currencies such as bitcoins. [Ransomware is one of the most widely used methods of attacks](https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise).

Ransomware enters computer networks and encrypts files using public-key encryption. Unlike other malware, this encryption key stays on the cyber criminal’s server. Cyber criminals will request ransom for this private key. Cyber criminals are using encryption as a weapon to hold the data hostage.

Ransomware is hard to detect before it’s too late, and ransomware techniques continue to evolve. Because of this, your institution should focus on prevention efforts. Prevention efforts include training for employees and strong information security controls.

The DOB recommends developing strong business continuity plans and incident response plans. Plan development may help in the event of a ransomware attack.

## Distributed Denial of Service (DDoS) Attacks

DDoS attacks make an online service unavailable by overwhelming it with excessive traffic from many locations and sources. Website response time slows down, preventing access during a DDoS attack. Cyber criminals develop large networks of infected computers called Botnets by planting malware. A DDoS attack may not be the primary cyber crime. The attacks often create a distraction while other types of fraud and cyber intrusion are attempted.

The Federal Financial Institutions Examination Council (FFIEC) issued a [joint statement on DDoS attacks, risk mitigation, and additional resources](https://www.ffiec.gov/press/PDF/FFIEC%20DDoS%20Joint%20Statement.pdf).

## Spam & Phishing

Spam includes unwanted, unsolicited, or undesirable messages and emails. Phishing is a form of social engineering, including attempts to get sensitive information. Phishing attempts will appear to be from a trustworthy person or business.

Cyber criminals pretend to be an official representative sending you an email or message with a warning related to your account information. The message will often ask for a response by following a link to a fake website or email address where you will provide confidential information. The format of the message will typically appear legitimate using proper logos and names. Any information entered into the fake link goes to the cyber criminal.

The FBI developed [tips for preventing phishing attacks](https://archives.fbi.gov/archives/news/stories/2009/april/spearphishing_040109).

## Corporate Account Takeover (CATO)

CATO is a business entity theft where cyber thieves impersonate the business and send unauthorized wire and ACH transactions.  The unauthorized funds are sent to accounts controlled by the cyber criminal.

Many businesses are vulnerable to a CATO attack. Institutions with weak computer safeguards and minimal controls over online banking systems are easy targets. This form of cyber crime can result in large losses. Cyber criminals use malware to infect a computer through e-mail, websites, or malware disguised as software.

The Conference of State Bank Supervisors (CSBS) developed a [CATO best practices document](https://www.csbs.org/ec/cato/Documents/BestPracticesCATO.docx).

## Automated Teller Machine (ATM) Cash Out

ATM Cash Out is a type of large dollar value ATM fraud. Cash-outs involve simultaneous large cash withdrawals from several ATMs in many regions. It may also include large withdrawals at one ATM.

The Cash Out usually affects small-to medium-sized financial institutions. The attack involves changing the settings on ATM web-based control panels. Cyber criminals change the ATM's dispense function control to "Unlimited Operations." The “Unlimited Operations" setting allows withdrawal of funds over the customer's account balance or beyond the ATM’s cash limit. Stolen ATM or debit card information is often used to withdraw the funds. As a result, your financial institution can suffer large dollar losses.

The DOB recommends reviewing your control over information technology networks, card issuer authorization systems, systems that manage ATM parameters, and fraud detection and response processes to prevent ATM Cash Out attacks.

Roles and Responsibilities

## **IT Security Roles and Responsibilities**

Here are some of the vital IT security roles and the responsibilities associated with them. Don’t be surprised that sometimes, different roles share some responsibilities. After all, cybersecurity requires a complex approach from professionals working in this field.

### **Application Security Engineer**

The job of an app security engineer has two major aspects. Firstly, you will need to help developers to create more secure apps. Secondly, you’ll need to control [third-party apps](https://spinbackup.com/blog/third-party-apps-audit-data-protection/) used by your company and ensure their safety. Some of the typical responsibilities and tasks include:

* Configuring technical security controls
* Conducting an app risk assessment
* Whitelisting/blacklisting apps
* Performing penetration testing

For app security engineers, it’s vital to control SaaS apps and the risks related to them. [Risky and insecure apps](https://spinbackup.com/blog/fake-apps-definition-and-protection/) should be blacklisted. To automate your job and remain time-efficient, you’ll probably need specialized software that helps you with [app security assessment](https://spinbackup.com/blog/spinone-application-auditing-capabilities/) and whitelisting/blacklisting. Here’s how our solution helps with these tasks:

### **CISO**

A CISO (Chief Information Security Officer) is a C-level employee whose task is to oversee corporate security strategy. The typical CISO’s responsibilities include:

* Planning long-term security strategy
* Planning and implementing data loss prevention measures
* Managing access
* Ensuring that the company implements proper safeguards to meet compliance requirements
* Investigating any incidents and preventing them in the future
* Assessing security risk
* Arranging security awareness training

### **Data Protection Officer**

Having a DPO is one of the [GDPR compliance requirements](https://spinbackup.com/blog/gdpr-compliance/). A DPO must be appointed in organizations working with large-scale systematic monitoring or processing of sensitive data. Officers oversee corporate data protection measures and their effectiveness.  A specialist, appointed to the DPO role, controls whether corporate security is of a sufficient level to meet compliance requirements, and recommends security upgrades if needed. That’s why an in-depth understanding of data security and compliance are essential skills. You can read more about the role of DPO here.

***Read more about***[***DPO role and responsibilities here.***](https://spinbackup.com/blog/the-role-of-data-protection-officer-in-gdpr-compliance/)

### **Network Security Engineer**

As the name suggests, a network security engineer’s job is to protect corporate networks from data breaches, human error, or cyberattacks. Engineers are responsible for:

* Configuring network security settings
* Performing penetration testing
* Developing and implementing sufficient measures to detect [cyber threats](https://spinbackup.com/blog/types-of-cyber-security-threats/)
* Implementing network security policies
* Installing and maintaining security software like firewalls

### **Security Administrator**

An IT security admin is a role that includes a wide range of skills and responsibilities to manage the protection of the company’s data. Some of the most common admin’s responsibilities include:

* Managing access
* Ensuring that [data migration](https://spinbackup.com/blog/how-to-migrate-google-data/) is secure
* Configuring security software
* Monitoring [data behavior for abnormal activities](https://spinbackup.com/blog/spinone-domain-audit-capabilities/)
* Implementing security policies
* Testing company’s systems to locate [potential risks](https://spinbackup.com/blog/biggest-cloud-computing-risks/) and vulnerabilities
* Reporting security statuses and incidents (if any)
* Using [software tools](https://spinbackup.com/products/gsuite-security/) to automate some of the tasks

An admin’s role is more significant than it may seem at first glance. An admin has to keep the whole organization’s security landscape in mind and ensure that even the tiniest processes are executed correctly. After all, even one careless click may be enough to initiate a cyberattack.

### **Security Analyst**

What is the role of an information security analyst? This role is related to protecting corporate information against [cyberattacks and insider threats](https://spinbackup.com/blog/types-of-cyber-security-threats/). Generally, an analyst has to determine potential risks and vulnerabilities inside the system, so a deep understanding of data security threats and ways to prevent them is a must. As a security analyst, your responsibilities will include:

* Analyzing and configuring corporate systems to improve their security
* Analyzing data loss prevention measures
* Looking for system vulnerabilities and ways to fix them
* Monitoring data behavior for abnormal activities
* Verifying security, availability, and confidentiality of corporate data

Also, the security analyst’s role requires an understanding of [white hat hacking](https://spinbackup.com/blog/45-main-cybersecurity-terms-everyone-must-know/#Hacking_and_Social_Engineering) to design more advanced protection against cyberattacks. Analysts often work together with security architects.

### **Security Architect**

A security architect is one of the senior-level IT security positions. An architect is focused on creating a secure-by-design environment. Unsurprisingly, this position requires a solid understanding of network, app, and hardware security, as well as experience with various systems. Generally, an architect’s responsibilities include:

* Assessing the system’s security controls and processes to find potential security gaps
* Planning changes and upgrades for corporate IT infrastructure
* Maintaining system integrity
* Implementing [insider threat control](https://spinbackup.com/blog/g-suite-security-insider-threat-control-dlp/) measures
* Choosing new security software if needed
* Implementing [disaster recovery](https://spinbackup.com/blog/disaster-recovery-plan/) measures
* Analyzing previous incidents and creating an incident response plan
* Analyzing the [costs and benefits of security solutions](https://spinbackup.com/blog/the-cost-of-data-breach/)

Of course, the exact scope of your tasks as an architect will vary depending on each organization’s unique infrastructure and needs. Often, an architect needs to assess corporate systems for meeting security compliance standards like [HIPAA](https://spinbackup.com/blog/how-spinone-helps-you-to-meet-hipaa-compliance-requirements/) or [NIST](https://spinbackup.com/blog/how-spinone-helps-you-to-meet-nist-800-171-compliance-requirements/) to decide what changes are needed to become compliant.

**Read more about** [***compliance in the cloud systems***](https://spinbackup.com/blog/compliance-guide-for-public-cloud/)**.**

### Security Specialist

An IT security specialist is a person responsible for keeping corporate data safe. Security specialists maintain and upgrade systems and procedures to prevent data loss or leakage. IT specialists have many sub-specializations. Depending on a specific environment, an information security specialist will have a stronger focus on cloud, network, app, database, SCADA, or device security.    In some cases, especially in small businesses, an IT security specialist is an all-rounder with responsibilities combining many cybersecurity roles at the same time. That’s why a security specialist must have strong IT skills and a deep understanding of both software and hardware—and, of course, an ability to locate potential vulnerabilities and fix them.