SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

AN AUTONOMOUS INSTITUTION

Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

UNIT-V MANAGEMENT AND INCIDENTS

Security Planning

A security plan is a document that describes how an organization will address its security needs. The plan is subject to periodic review and revision as the organization's security needs change.Enterprise security starts with a security plan that describes how an organization will address its security needs.

Organizations and Security Plans

A good security plan is an official record of current security practices, plus a blueprint for orderly change to improve those practices. By following the plan, developers and users can measure the effect of proposed changes, leading eventually to further improvements. The impact of the security plan is important, too. A carefully written plan, supported by management, notifies employees that security is important to management (and therefore to everyone). Thus, the security plan has to have appropriate content and has to produce desired effects.

Contents of a Security Plan

A security plan identifies and organizes the security activities for a computing system. The plan is both a description of the current situation and a map for improvement. Every security plan must address seven issues:

- policy, indicating the goals of a computer security effort and the willingness of the people involved to work to achieve those goals
- current state, describing the status of security at the time of the plan
- requirements, recommending ways to meet the security goals
- recommended controls, mapping controls to the vulnerabilities identified in the policy and requirements
- accountability, documenting who is responsible for each security activity
- timetable, identifying when different security functions are to be done
- maintenance, specifying a structure for periodically updating the security plan

Security Planning Team Members

The membership of a computer security planning team must somehow relate to the different aspects of computer security described in this book. Security in operating systems and networks requires the cooperation of the systems administration staff. Program security measures can be understood and recommended by applications programmers. Physical security controls are implemented by those responsible for general physical security, both against human attacks and natural disasters. Finally, because controls affect system users, the plan should incorporate users' views, especially with regard to usability and the general desirability of controls.

Thus,no matter how it is organized, a security planning team should represent each of the following groups.

- computer hardware group
- system administrators
- systems programmers
- applications programmers
- data entry personnel
- physical security personnel
- representative users

Assuring Commitment to a Security Plan

After the plan is written, it must be accepted and its recommendations carried out. Acceptance by the organization is key: A plan that has no organizational commitment is simply a plan that collects dust on the shelf. Commitment to the plan means that security functions will be implemented and security activities carried out. Three groups of people must contribute to making the plan a success.

- The planning team must be sensitive to the needs of each group affected by the plan.
- Those affected by the security recommendations must understand what the plan means for the way they will use the system and perform their business activities. In particular, they must see how what they do can affect other users and other systems.
- Management must be committed to using and enforcing the security aspects of the system.

Business Continuity Planning

Small companies working on a low profit margin can be put out of business by a computer incident. Large, financially sound businesses can weather a modest incident that interrupts their use of computers for a while, although it is painful to them. But even rich companies do not want to spend money unnecessarily. The analysis is sometimes as simple as no computers means no customers means no sales means no profit.

Government agencies, educational institutions, and nonprofit organizations also have limited budgets, which they want to use to further their needs. They may not have a direct profit motive, but being able to meet the needs of their customers—the public, students, and constituents—partially determines how well they will fare in the future. All kinds of organizations must plan for ways to cope with emergency situations.

A business continuity plan documents how a business will continue to function during or after a computer security incident. An ordinary security plan covers computer security during normal times and deals with protecting against a wide range of vulnerabilities from the usual sources. A business continuity plan deals with situations having two characteristics:

- catastrophic situations, in which all or a major part of a computing capability is suddenly unavailable

- long duration, in which the outage is expected to last for so long that business will suffer

A business continuity plan would be helpful in many situations. Here are some examples that typify what you might find in reading your daily newspaper:

- A fire destroys a company’s entire network.

- A seemingly permanent failure of a critical software component renders the computing system unusable.

- The abrupt failure of a supplier of electricity, telecommunications, network access, or other critical service limits or stops activity.

- A flood prevents the essential network support staff from getting to the operations center.

Assess Business Impact

To assess the impact of a failure on your business, you begin by asking two key questions:

- What are the essential assets? What are the things that if lost will prevent the business from doing business? Answers are typically of the form “the network,” “the customer reservations database,” or “the system controlling traffic lights.”

- What could disrupt use of these assets? The vulnerability is more important than the threat agent. For example, whether destroyed by a fire or zapped in an electrical storm, the network is nevertheless down. Answers might be “failure,” “corrupted,” or “loss of power.”

Develop Strategy

The continuity strategy investigates how the key assets can be safeguarded. In some cases, a backup copy of data or redundant hardware or an alternative manual process is good enough. Sometimes, the most reasonable answer is reduced capacity. The result of a strategy analysis is a selection of the best actions, organized by circumstances. The strategy can then be used as the basis for your business continuity plan.

Develop the Plan

The business continuity plan specifies several important things:

- who is in charge when an incident occurs

- what to do

- who does it

The plan justifies making advance arrangements, such as acquiring redundant equipment, arranging for data backups, and stockpiling supplies, before the catastrophe. The plan also justifies advance training so that people know how they should react. In a catastrophe there will be confusion; you do not want to add confused people to the already severe problem.

The focus of the business continuity plan is to keep the business going while someone else addresses the crisis. That is, the business continuity plan does not include calling the fire department or evacuating the building, important though those steps are. The focus of a business continuity plan is the business and how to keep it functioning to the degree possible in the situation. Handling the emergency is someone else’s problem.

Handling Incidents

Individuals must take responsibility for their own environments. But students in a university or employees of a company or government agency sometimes assume it is someone else's responsibility. Or they don't want to bother a busy operations staff with something that may be nothing at all. Organizations develop a capability to handle incidents from receiving the first report and investigating it. In this section we consider incident handling practices.

Incident Response Plans

A (security) incident response plan tells the staff how to deal with a security incident. In contrast to the business continuity plan, the goal of incident response is handling the current security incident, without direct regard for the business issues. The security incident may at the same time be a business catastrophe, as addressed by the business continuity plan. But as a specific security event, it might be less than catastrophic (that is, it may not severely interrupt business) but could be a serious breach of security, such as a hacker attack or a case of internal fraud. An incident could be a single event, a series of events, or an ongoing problem.

An incident response plan should

- define what constitutes an incident

- identify who is responsible for taking charge of the situation

- describe the plan of action The plan usually has three phases: advance planning, triage, and running the incident. A fourth phase, review, is useful after the situation abates so that this incident can lead to improvement for future incidents.

Incident Response Teams

Many organizations name and maintain a team of people trained and authorized to handle a security incident. Such teams, called computer security incident response teams (CSIRTs) or computer emergency response teams (CERTs) are standard at large private and government organizations, as well as many smaller ones. A CSIRT can consist of one person or it can be a flexible team of dozens of people on call for special skills they can contribute.

Here are some models for CSIRTs:

- a full organizational response team to cover all incidents; such a team may include separate staff to deal with situations in different organizational units, such as plants in separate locations or distinct business units of a larger company

- coordination centers to coordinate incident response activity across organizations, so that work is not duplicated unnecessarily and efforts proceed toward the same goals

- so-called national CSIRTs with coordination responsibility within a country and to national CSIRTs of other countries

- sector CSIRTs to assist with investigating and handling incidents specific to a particular business sector, for example, financial institutions or medical facilities; some attacks focus on one type of target (for example, in 2013 large banks were the target of massive denial-of-service attacks)

- vendor CSIRTs to address or participate in incidents involving one manufacturer's products

- outsourced CSIRT teams, hired to perform incident response services on contract to other companies

Risk Analysis

Risk analysis is an organized process for identifying the most significant risks in a computing environment, determining the impact of those risks, and weighing the desirability of applying various controls against those risks.Good, effective security planning includes a careful risk analysis. A risk is a potential problem that the system or its users may experience.

- A loss associated with an event. The event must generate a negative effect: compromised security, lost time, diminished quality, lost money, lost control, lost understanding, and so on. This loss is called the risk impact.

- The likelihood that the event will occur. The probability of occurrence associated with each risk is measured from 0 (impossible) to 1 (certain). When the risk probability is 1, we say we have a problem.

- The degree to which we can change the outcome. We must determine what, if anything, we can do to avoid the impact or at least reduce its effects. Risk control involves a set of actions to reduce or eliminate the risk. Many of the security controls we describe in this book are examples of risk control.

We usually want to weigh the pros and cons of different actions we can take to address each risk. To that end, we can quantify the effects of a risk by multiplying the risk impact by the risk probability, yielding the **risk exposure.**

Risk is inevitable in life: Crossing the street is risky but that does not keep us from doing it. We can identify, limit, avoid, or transfer risk but we can seldom eliminate it. In general, we have three strategies for dealing with risk:

- avoid the risk by changing requirements for security or other system characteristics

- transfer the risk by allocating the risk to other systems, people, organizations, or assets; or by buying insurance to cover any financial loss should the risk become a reality

- assume the risk by accepting it, controlling it with available resources and preparing to deal with the loss if it occurs

Risk leverage is the difference in risk exposure divided by the cost of reducing the risk.

Risk analysis is the process of examining a system and its operational context to determine possible exposures and the potential harm they can cause. Thus, the first step in a risk analysis is to identify and list all exposures in the computing system of interest.

Arguments For and Against Risk Analysis

Risk analysis is a well-known planning tool, used often by auditors, accountants, and managers. In many situations, such as obtaining approval for new drugs, new power plants, and new medical devices, a risk analysis is required by law in many countries. There are many good reasons to perform a risk analysis in preparation for creating a security plan.

- Improve awareness. Discussing issues of security can raise the general level of interest and concern among developers and users. Especially when the user population has little expertise in computing, the risk analysis can educate users about the role security plays in protecting functions and data that are essential to user operations and products.

- Relate security mission to management objectives. Security is often perceived as a financial drain for no gain. Management does not always see that security helps balance harm and control costs.

- Identify assets, vulnerabilities, and controls. Some organizations are unaware of their computing assets, their value to the organization, and the vulnerabilities associated with those assets. A systematic analysis produces a comprehensive list of assets, valuations, and risks.

- Improve basis for decisions. A security manager can present an argument such as “I think we need a firewall here” or “I think we should use token-based authentication instead of passwords.” Risk analysis augments the manager’s judgment as a basis for the decision.

- Justify expenditures for security. Some security mechanisms appear to be very expensive and without obvious benefit. A risk analysis can help identify instances where it is worth the expense to implement a major security mechanism. Managers can show the much larger risks of not spending for security.

However, despite the advantages of risk analysis, there are several arguments against using it to support decision making.

- False sense of precision and confidence. The heart of risk analysis is the use of empirical data to generate estimates of risk impact, risk probability, and risk exposure. The danger is that these numbers will give us a false sense of precision, thereby giving rise to an undeserved confidence in the numbers. However, in many cases the numbers themselves are much less important than their relative sizes. Whether an expected loss is $100,000 or $150,000 is relatively unimportant. It is much more significant that the expected loss is far above the $10,000 or $20,000 budget allocated for implementing a particular control. Moreover, anytime a risk analysis generates a large potential loss, the system deserves further scrutiny to see if the root cause of the risk can be addressed.

- Hard to perform. Enumerating assets, vulnerabilities, and controls requires creative thinking. Assessing loss frequencies and impact can be difficult and subjective. A large risk analysis will have many things to consider. Risk analysis can be restricted to certain assets or vulnerabilities, however.

- Immutability. Many software project leaders view processes like risk analysis as an irritating fact of life—a step to be taken in a hurry so that the developers can get on with the more interesting jobs related to designing, building, and testing the system. For this reason, risk analyses, like contingency plans and five-year plans, have a tendency to be filed and promptly forgotten. But if an organization takes security seriously, it will view the risk analysis as a living document, updating it at least annually or in conjunction with major system upgrades.

- Lack of accuracy. Risk analysis is not always accurate, for many reasons. First, we may not be able to calculate the risk probability with any accuracy, especially when we have no past history of similar situations. Second, even if we know the likelihood, we cannot always estimate the risk impact very well. The risk management literature is replete with papers about describing the scenario, showing that presenting the same situation in two different ways to two equivalent groups of people can yield two radically different estimates of impact. And third, we may not be able to anticipate all the possible risks.

Dealing with Disaster

Dealing with nontechnical problems has two aspects: preventing things that can be prevented and recovering from the things that cannot be prevented. Physical security is the term used to describe protection needed outside the computer system. Typical physical security controls include guards, locks, and fences to deter direct attacks. In addition, there are other kinds of protection against less direct disasters, such as floods and power outages; these, too, are part of physical security.

Natural Disasters

Computers are subject to the same natural disasters that can occur to homes, stores, and automobiles. They can be flooded, burned, melted, hit by falling objects, and destroyed by earthquakes, storms, and tornadoes. Additionally, computers are sensitive to their operating environment, so excessive heat or inadequate power is also a threat. No one can prevent natural disasters, but through careful planning, organizations can reduce the damage they inflict. Some measures can be taken to reduce their impact. Because many of these perils cannot be prevented or predicted, controls focus on limiting possible damage and recovering quickly from a disaster. Issues to be considered include the need for offsite backups, the cost of replacing equipment, the speed with which equipment can be replaced, the need for available computing power, and the cost or difficulty of replacing data and programs.

Power Loss

Computers need their food—electricity—and they require a constant, pure supply of it. With a direct power loss, all computation ceases immediately. Because of possible damage to media by sudden loss of power, many disk drives monitor the power level and quickly retract the recording head if power fails. For certain time-critical applications, loss of service from the system is intolerable; in these cases, alternative complete power supplies must be instantly available.

Surge Suppressor

Another problem with power is its “cleanness.” Although most people are unaware of it, a variation of 10 percent from the stated voltage of a line is considered acceptable, and some power lines vary even more. A particular power line may consistently be up to 10 percent high or low. In many places, lights dim momentarily when a large appliance, such as an air conditioner, begins operation. When a large motor starts, it draws an exceptionally large amount of current, which reduces the flow to other devices on the line. When a motor stops, the sudden termination of draw can send a temporary surge along the line. Similarly, lightning strikes may send a momentary large pulse. Thus, instead of being constant, the power delivered along any electric line shows many brief fluctuations, called drops, spikes, and surges. A drop is a momentary reduction in voltage, and a spike or surge is a rise. For computing equipment, a drop is less serious than a surge. Most electrical equipment is tolerant of rather large fluctuations of current

Human Vandals

Because computers and their media are sensitive to a variety of disruptions, a vandal can destroy hardware, software, and data. Human attackers may be disgruntled employees, bored operators, saboteurs, people seeking excitement, or unwitting bumblers. If physical access is easy to obtain, crude attacks using axes or bricks can be very effective. One man recently shot a computer that he claimed had been in the shop for repairs many times without success.

Physical attacks by unskilled vandals are often easy to prevent; a guard can stop someone approaching a computer installation with a threatening or dangerous object. When physical access is difficult, more subtle attacks can be tried, resulting in quite serious damage. People with modest technical knowledge of a system can short-circuit a computer with a car key or disable a disk drive with a paper clip. These items are not likely to attract attention until the attack is completed.

The Internet of Things

The Internet of things refers to the connection of everyday devices to the Internet, making a world of so-called smart devices. The cost of processors is low, and engineers envision being able to offer new products and services by embedding these processors in everyday devices. Consider these possibilities for Internet-enabled products:

- smart appliances. Your refrigerator can sense when you are running low on milk and add that to your electronic shopping list. Your dishwasher chooses a time to run when electrical demand is low, for example, in the middle of the night, to shift use away from times of peak demand.

- smart home. Your home security system reports to you when it senses an intrusion or anomaly. Your heating system coordinates with your calendar to reduce your thermostat when your calendar says you will be away.

- smart health. Your exercise monitor interacts with your treadmill to make your workouts more strenuous as your physical condition improves. Your glucose monitor sends reports to your doctor.

- smart transportation. Cars, trains, buses, and airplanes operate without human drivers, sensing adverse traffic conditions and rerouting public transportation (while simultaneously sending reports to waiting passengers advising them of revised arrival times and alternative pickup points).

- smart entertainment. Your video recorder predicts and records programs you will (or are likely to) want to watch. Your virtual concierge books tickets (and arranges a date for you) to attend a performance it infers you will like.

- smart computer. Your computer manages local and Internet-based data storage to optimize retrieval time and use of local resources. Your computer uses spare execution cycles to contribute to solving computation-intensive problems throughout the world.

Each of these applications seems to be a noble activity that at least some users would embrace. But with your security hat on, you might detect a negative side to each, for example:

- loss of privacy. Learning that you are not exercising as frequently or vigorously as it would like, your insurance company raises your premium.

- loss of control. You keep sensitive data on your computer. Your agreement for automatic backups initially involves only domestic storage of your data, but the backup company acquires a new foreign owner in a country whose data protection policies are not trustworthy.

- potential for subversion. A malevolent government influences the opinions of its citizens by controlling content provided through online news sources, by planting slanted or even false stories.

- mistaken identification. You share your computer with a houseguest who has different tastes in entertainment from you, so inappropriate programs are recorded and your favorites are not.

- uncontrolled access. The exchange between your thermostat and your calendar is intercepted by a third party who, realizing your home is vacant, burglarizes while you are away.

Economics

Security professionals must make a variety of security decisions about the computers, systems, or networks they design, build, use, and maintain. In this section, we focus on decisions involved in allocating scarce financial resources to cybersecurity. That is, you must decide what kinds of security controls to invest in, based on need, cost, and the tradeoffs with other investments (that may not be security related).

To make a convincing business case for security investment, we need data on the risks and costs of security incidents. Unfortunately, as our discussion shows, reliable data are hard to find, so we outline the kind of data collection that would help security professionals. Once we have good data, we can build models and make projections. Building and using a model involves understanding key factors and relationships; we discuss examples of each. Finally, we explore the possibilities for future research in this rich, interdisciplinary area.

A business case for a given expenditure is a proposal that justifies the use of resources. It usually includes the following items:

- a description of the problem or need to be addressed by the expenditure
- a list of possible solutions
- a list of constraints on solving the problem
- a list of underlying assumptions
- an analysis of each alternative, including risks, costs, and benefits
- a summary of why the proposed investment is good for the organization

The Economic Impact of Cybersecurity

Understanding the economic impact of cybersecurity issues—prevention, detection, mitigation, and recovery—requires models of economic relationships that support good decision making. However, realistic models must be based on data derived both from the realities of investment in cybersecurity and consequences of actual attacks. In this section, we describe the nature of the data needed, the actual data available for use by modelers and decision-makers, and the gap between ideal and real. For any organization, understanding the nature of the cybersecurity threat requires knowing at least the following elements:

- number and types of assets needing protection
- number and types of vulnerabilities that exist in a system
- number and types of likely threats to a system

Electronic Voting

A good security engineer investigating what makes for good voting can point out the C-I-A requirements in the electoral process:

- Confidentiality. We want to be able to cast a ballot without revealing our votes to others.
- Integrity. We want votes to represent our actual choices, and not be changed between the time we mark the ballot and the time our vote is counted. We also want every counted ballot to reflect one single vote of an authorized person. That is, we want to be able to ensure that our votes are authentic and that the reported totals accurately reflect the votes cast.

- Availability. Usually, votes are cast during an approved pre-election period or on a designated election day, so we must be able to vote when voting is allowed. If we miss the chance to vote or if voting is suspended during the designated period, we lose the opportunity to cast a vote in the given election.

What Is Electronic Voting?

Electronic voting (sometimes called e-voting) refers to an election process that is partially or completed automated. In other words, electronic means are provided for casting votes, counting votes, or both. Thus, you may see the phrase used in different ways, depending on the implied meaning. In this book, we use the phrase to mean complete automation of the voting process from end to end. Note, however, that other people focus on specific activities in the voting process (maintaining lists of registered voters or transmitting votes from a voting booth to a central tabulation facility) that could be done electronically. In particular, casting votes on the Internet has popular appeal, and so some people look at that as electronic voting.

What Is a Fair Election?

We often hear about the need for "free and fair elections." But what exactly is a fair election?

a fair election is one that satisfies all of the following conditions:

- Each voter's choices must be kept secret.

- Each voter may vote only once and only for allowed offices.

- The voting system must be tamperproof, and the election officials must be prevented from allowing it to be tampered with.

- All votes must be reported accurately.

- The voting system must be available for use throughout the election period.

- An audit trail must be kept to detect irregularities in voting, but without disclosing how any individual voted.

Cyber Warfare

Cyber warfare is larger than cyber mischief, cybercrime, cyber espionage, cyber terrorism, or cyber attack. "Warfare" is a term typically reserved for active conflict between nation states.

When Is It Warfare?

What constitutes an act of war? According to some historians of war, the action must be taken by uniformed members of the attacking country's military, and the result must be acknowledged as a military action by the attacked country. By this standard, the attack on Estonia was not an act of war. It may have been instigated by organized criminals or a group of angry citizens, and it was not acknowledged as a military action by any national government.

How Likely Is It?

there will never be a true cyber war. They offer several reasons, including the difficulties of predicting the true effects of a cyber attack: "On the one hand [attacks] may be less powerful than hoped but may also have more extensive outcomes arising from the interconnectedness of systems, resulting in unwanted damage to perpetrators and their allies. More importantly, there is no strategic reason why any aggressor would limit themselves to only one class of weaponry."

At the same time, they point to the proliferation of cyber weaponry: "Cyberweapons are used individually, in combination and also blended simultaneously with conventional 'kinetic' weapons as force multipliers. It is a safe prediction that the use of cyberweaponry will shortly become ubiquitous." Cyber weapons act like conventional ones: They destroy or disrupt a population's ability to function, weaken the economy, and devastate morale. However, whereas a bomb destroying a bridge or factory can lead to a long recovery time, electronic equipment is fungible and easily replaced. Cyber conflict may shut down a network, but network connectivity and routing have been designed for resilience, so recovery can be reasonably fast.

What Are Appropriate Reactions to Cyber War?

It is difficult to prepare for cyber war, because there are few precedents. "Governments know how to negotiate treaties and engage in diplomacy to head off conventional wars, but no one really knows how a confrontation between nations would escalate into a cyberwar,"

Some governments are considering increased monitoring of activities on the cyber infrastructure, as a way of watching for unwelcome behavior. But civil liberties organizations are urging care in implementing monitoring.

What is Cyberspace?

We have all seen that technology is a great leveler. Using technology, we created machine-clones – computers, which are high-speed data processing devices.

They can also manipulate electrical, magnetic, and optical impulses to perform complex arithmetic, memory, and logical functions. The power of one computer is the power of all connected computers termed as a network-of-network or the internet.

Cyberspace is the dynamic and virtual space that such networks of machine-clones create. In other words, cyberspace is the web of consumer electronics, computers, and communications network which interconnect the world.

Cyberspace vs. Physical World

Firstly, cyberspace is a digital medium and not a physical space. It is an interactive world and is not a copy of the physical world. Here are some differences between cyberspace and the physical world:

Physical World	Cyberspace
Static, well-defined, and incremental	Dynamic, undefined, and exponential

Has fixed contours	Is as vast as the human imagination and has no fixed shape

In a human brain, there are countless neurons which create a spectre of life. Similarly, the cyberspace represents millions of computers creating a spectre of digital life. Therefore, cyberspace is a natural extension of the physical world into an infinite world.

Cyber Security and Cyber Laws

As technology evolved, the need to regulate human behavior evolved too. Cyber laws came into existence in order to ensure that people use technology and avoid its misuse.

If an individual commits an act which violates the rights of a person in the cyberspace, then it is treated as a cyberspace violation and punishable under the provisions of the cyber laws.

Since the cyberspace is completely different from the physical world, traditional laws are not applicable here. In order to provide cyber security to users, the government introduced several cyber laws.

When the internet was designed and developed, the developers had no idea that it would have the potential of growing to such great an extent.

Today, many people are using the internet for illegal and immoral activities which need regulation. In the cyberspace things like money laundering, identity theft, terrorism, etc. have created a need for stringent laws to enhance cybersecurity.

Additionally, many technologically qualified criminals like hackers interfere with internet accounts through the Domain Name Server (DNS), IP address, phishing, etc. and gain unauthorized access to a user's computer system and steal data.

While there is no clear definition of cyber law, it is broadly the legal subject which emanated from the development of technology, innovation of computers, use of the internet, etc.

Cyber Law

Cyber Law encapsulates legal issues which are related to the use of communicative, transactional, and distributive aspects of networked information technologies and devices.

It is not as distinct as the Property Law or other such laws since it covers many areas the law and regulation. It encompasses the legal, statutory, and constitutional provisions which affect computers and networks.

Further, it concerns itself with individuals, and institutions which:

- Play an important part in providing access to cyberspace
- Create hardware or software which allows people to access cyberspace
- Use their own computers and enter cyberspace

Cyber Law is a generic term referring to all the legal and regulatory aspects of the internet. Everything concerned with or related to or emanating from any legal aspects or concerning any activities of the citizens in the cyberspace comes within the ambit of cyber laws.

Currently, there are two main statutes which ensure cyber security:

1. The Indian Penal Code. 1860
2. The Information Technology Act, 2000

Cybercrime

A **cybercrime** is a crime that involves a computer or a computer network.The computer may have been used in committing the crime, or it may be the target. Cybercrime may harm someone's security or finances.

Computer crime encompasses a broad range of activities, including computer fraud, financial crimes, scams, cybersex trafficking, and ad fraud.

Computer fraud

Computer fraud is the act of using a computer to take or alter electronic data, or to gain unlawful use of a computer or system. If computer fraud involves the use of the Internet, it can be considered Internet fraud. The legal definition of computer fraud varies by jurisdiction, but typically involves accessing a computer without permission or authorisation.

Forms of computer fraud include hacking into computers to alter information, distributing malicious code such as computer worms or viruses, installing malware or spyware to steal data, phishing, and advance-fee scams.

Other forms of fraud may be facilitated using computer systems, including bank fraud, carding, identity theft, extortion, and theft of classified information. These types of crimes often result in the loss of private or monetary information.

Cyberterrorism

Cyberterrorism, in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources.Acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by means such as computer viruses, computer worms, phishing, malicious software, hardware methods, or programming scripts can all be forms of cyberterrorism.

Government officials and information technology security specialists have documented a significant increase in Internet problems and server scams since early 2001. Within the United States, there is a growing concern among government agencies such as the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) that such intrusions are part of an organized effort by cyberterrorist foreign intelligence services or other groups to map potential security holes in critical systems.

Cyberextortion

Cyberextortion is a type of extortion that occurs when a website, e-mail server, or computer system is subjected to or threatened with attacks by malicious hackers, such as denial-of-service attacks. Cyberextortionists demand money in return for promising to stop the attacks and to offer "protection". According to the Federal Bureau of Investigation, cybercrime extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate, and demanding payments to restore their service. More than 20 cases are reported each month to the FBI and many go unreported in order to keep the victim's name out of the public domain. Perpetrators typically use a distributed denial-of-service attack.[19] However, other cyberextortion techniques exist, such as doxing, extortion, and bug poaching.

Computer as a target

These crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes require the technical knowledge of the perpetrators. As such, as technology evolves, so too does the nature of the crime. These crimes are relatively new, having been in existence for only as long as computers have—which explains how unprepared society and the world, in general, are towards combating these crimes. There are numerous crimes of this nature committed daily on the internet. They are seldom committed by loners, instead usually involving large syndicate groups.

Crimes that primarily target computer networks include:

- Computer viruses
- Denial-of-service attacks
- Malware (malicious code)

Ad-fraud

Ad-frauds are particularly popular among cybercriminals, as such frauds are less likely to be prosecuted and are particularly lucrative cybercrimes.[41] Jean-Loup Richet, Professor at the Sorbonne Business School, classified the large variety of ad-fraud observed in cybercriminal communities into three categories: (1) identity fraud; (2) attribution fraud; and (3) ad-fraud services.[13]

Identity fraud aims to impersonate real users and inflate audience numbers. Several ad-fraud techniques relate to this category and include traffic from bots (coming from a hosting company or a data center, or from compromised devices); cookie stuffing; falsifying user characteristics, such as location and browser type; fake social traffic (misleading users on social networks into visiting the advertised website); and the creation of fake social signals to make a bot look more legitimate, for instance by opening a Twitter or Facebook account.