Asian School of Cyber Laws

Asian School of Cyber Laws has been audited under British Standard BS-7799: 2002 for management of information security.

# Computer Crime & Abuse Report (India) 2001-02

Published on 1 Mar 2003
Revised on 15 Mar 2003

## HIGHLIGHTS OF THE REPORT

This report analyzes 6266 incidents of computer crime and abuse from 1st January 2001 through 31st December, 2002

These incidents range from obscene, threatening and defamatory emails to computer aided sabotage, source code thefts and even attempted cyber murders !

Incidents were reported by the IT, Manufacturing, Financial services, Education, Telecom, Health care, Other Services and other sectors.

The types of computer crime and abuse incidents include data theft email abuse, unauthorized access, data alteration, targeted virus attacks, denial of service attacks.

**Some findings of the report:**

Almost 60% of computer crime incidents are likely to occur in the first six months of a year.

The occurrence of a computer crime incident is

- most likely in September
- least likely in August.
- more likely on a Monday, Friday or Saturday.
- Least likely on a Sunday

A disgruntled former employee is more likely to commit a computer crime than a business rival.

Two thirds of data theft incidents are attributable to employees (current as well as former).

The average cost of a data theft attack is Rs. 1.8 lakh, with the cost ranging between Rs 20,000 and Rs. 1.87 crore.

In 97% of incidents involving obscene emails, the victims are female employees.

55% of unauthorized access incidents were traced to persons within the victim organization.

**Contents**



**This report can be obtained from http://www.asianlaws.org/report0102.pdf**

# INTRODUCTION

The Computer Emergency Response Team of Asian School of Cyber Laws (ASCL-CERT) was established in late 1999 to enable corporate India to battle the ever-growing wave of computer crime and computer abuse. ASCL-CERT team consists of IT and legal professionals.

On behalf of the ASCL-CERT, we extend an invitation to IT, legal and other professionals to join us in our efforts against computer crime and abuse. To learn more on how you can work with ASCL-CERT, please email us at cert@asianlaws.org.

Asian School of Cyber Laws (ASCL) is the pioneering institute in the field of education, training and consultancy in cyber law, cyber crime investigation and information security. In these fields ASCL works with several Universities and Colleges, Government departments, law enforcement agencies, defense organizations and corporates.

ASCL has been at the forefront of judicial activism by taking a keen interest in matters relating to public interest. Accordingly, ASCL students have filed Public Interest Litigations to rectify piquant situations arising out of various executive and legislative shortcomings.

The recent Central Government order to appoint Adjudicating Officers for cyber crimes was the outcome of a public interest litigation filed by ASCL in the Bombay High Court. Other issues that have been highlighted by ASCL and its students include online gambling, cyber pornography, defects in the digital signature law of India, etc.

# SCOPE OF THIS REPORT

The statistics in this report are based on 6266 incidents of computer crime and computer abuse reported to ASCL-CERT from January 1, 2001 through December 31, 2002, averaging over 8 incidents a day. These incidents range from obscene, threatening and defamatory emails to computer aided sabotage, source code thefts and attempted cyber murders.

Specifically, virus related incidents have been omitted if the source of the virus was "from the wild" i.e. unidentified and from the Internet. Only those virus-related incidents where the virus attack was attributed to an identified malicious attacker (e.g. a former employee, business rival etc) have been included in this report.

Those incidents that have been reported to the law enforcement authorities have not been included in this report since those matters are sub-judice and any comment on them would be inappropriate.

To maintain the privacy of the organizations and persons who provided the inputs for this report, they are only identified by the industry they represent.

This report does not aim to offer professional advise on the security technologies and methodologies available today.

Any recommendations and comments on the statistics are attributed to the Editorial Committee of the ASCL-CERT and do not reflect the official policies of the ASCL-CERT.

Asian School of Cyber Laws has been audited under British Standard BS-7799: 2002 for management of information security.

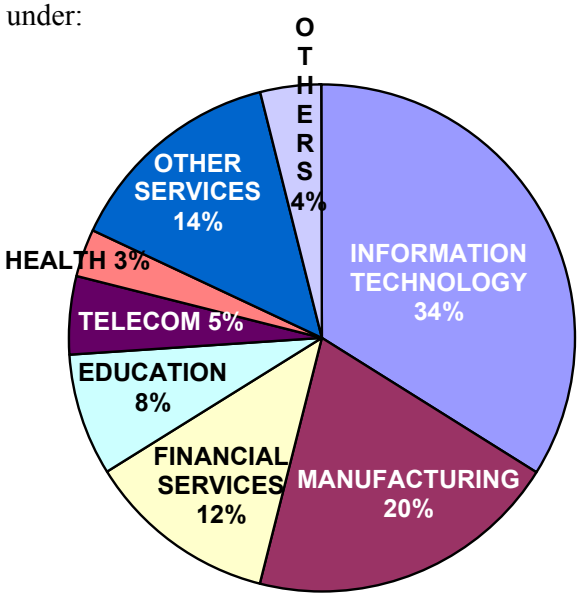
Most of our security policies can be obtained from http://www.asianlaws.org/policies

## SOURCES OF INFORMATION

In 2001-02, the ASCL-CERT interacted with over 600 small, medium and large-scale organizations from a wide spectrum of industries.

The interaction included but was not restricted to receiving details of incidents of computer crime and computer abuse witnessed by these organizations, advising them on how the perpetrators of the incidents could be identified and detailed recommendations on the methodology and mechanism to thwart similar incidents in the future.

The sector wise break up of organizations from whom the statistics were collected is illustrated as under:




**NOTE:** The **Information Technology sector** included hardware and software manufacturers, dealers and vendors; IT enabled services providers, E-commerce units, IT training institutes etc.

The **Other Services** sector includes insurance, transport, travel and tourism, consultants, and other service providers excluding financial services, IT and telecommunications.

The **Financial services** sector included banks, investment companies, brokerage houses etc.

The **Education sector** included Universities, colleges and training institutes.

## FINDINGS OF THE REPORT

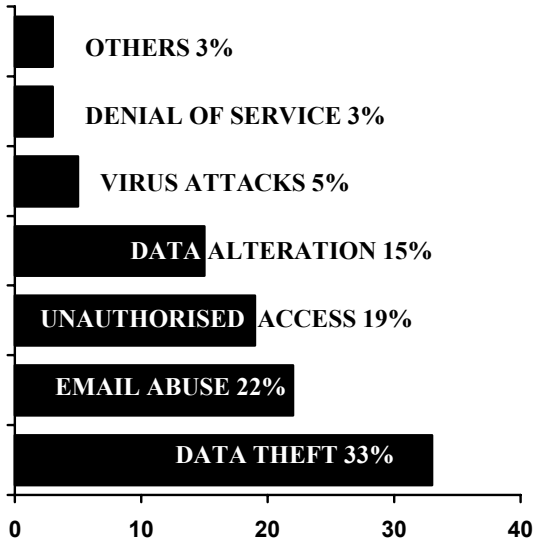
The findings of the report have been analysed on the basis of:

- types of incidents reported
- month wise and day wise breakup of incidents
- perpetrator wise breakup of incidents

### TYPES OF INCIDENTS

The computer crimes and abuses have been categorized into unauthorized access, data theft, email abuse, unauthorized access, data alteration, virus attacks, denial of service attacks (DoS), and others.

The break up of incidents is illustrated below:




**NOTE:** Unauthorized access incidents are those where there was no actual or suspected data theft.

Other incidents included web-defacement.

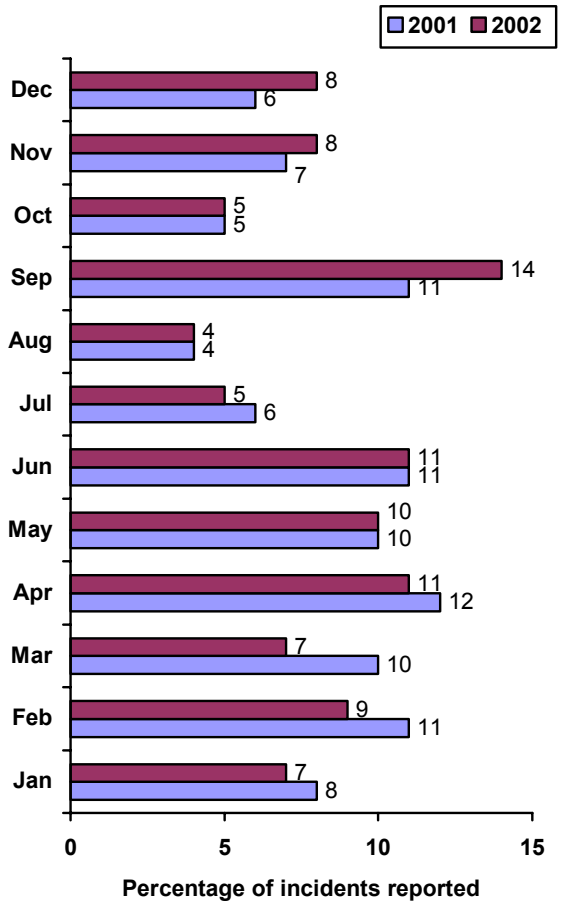
# MONTH / DAY-WISE BREAKUP

An analysis of the incidents that were reported, based on the month in which the incident was reported, shows an interesting trend.

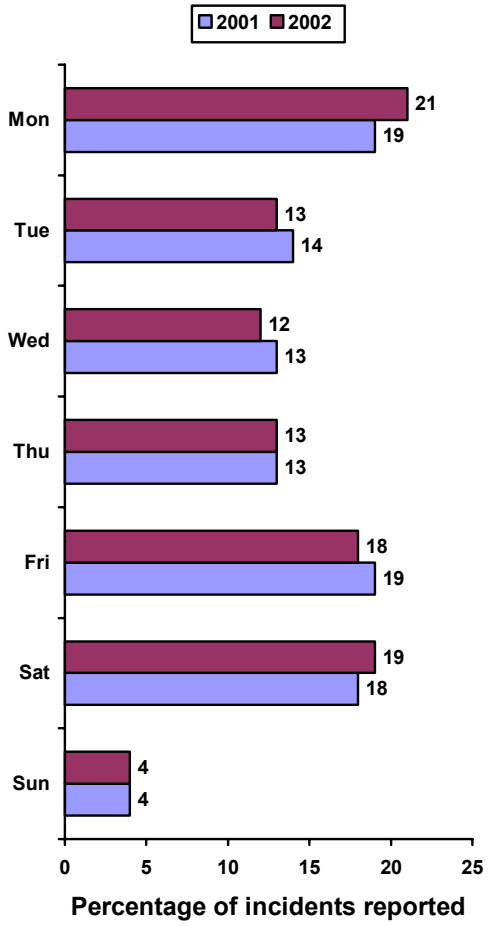
Overall, significantly more incidents (58.5%) were reported in the first six months of the year (i.e. from January to June) compared to the last six months (41.5%)

This disparity was more marked in 2001 when the first six months saw 62% of the incidents being reported as compared to 38% being reported in the last six months.

September topped the list with 11% in 2001 and 14% in 2002. August showed the least number of incidents with 4% in 2001 as well as 2002.




An analysis of the incidents that were reported, based on the day on which the incident was reported, also follows an interesting pattern.




More incidents are reported on Mondays, Fridays and Saturdays. These three days account for 57% of the incidents while the balance 43% were spread over the other four days.

Sundays accounted for the least number of incidents with the figure being 4% in 2001 and 2002.

# PERPETRATOR WISE BREAKUP

Overall, 21% of the reported incidents were traced back to employees, while 31% were traced to former employees of the victim organization.

Business rivalry was another major factor with 29% of the reported incidents being traced to rival organizations.

The balance, 19% of the incidents were such that the role, active or otherwise, of employees, former employees and rivals was not suspected.

These attacks were then classified into those suspected to be the handiwork of hackers (11%) and those suspected to have been carried out by script kiddies (8%).

The distinction was made on the basis of the tools used for the incident, the damage (actual and potential) and the methodology.

Those attacks where sophisticated techniques and methodologies were used have been classified as "hackers" incidents while the others have been classified as "script kiddies" attacks.

The term "script kiddies" implies the use of ready made "hacking scripts and codes" by "kids". Thousands of "underground" websites have sprung up that offer free download of hacking tools and utilities. Such tools are increasingly being used by youngsters for committing computer crimes.

It is interesting to note that the percentage of incidents attributable to former employees outnumbers those attributable to business rivals.

Another interesting fact is that more than half the incidents (52%) are attributable to employees (current as well as former).

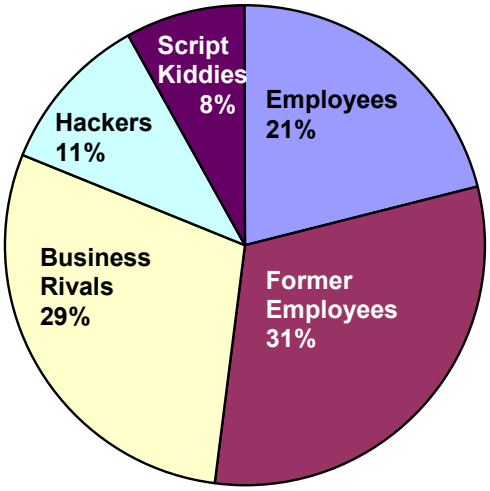
Most organizations were not forthcoming on the action taken against erring employees.

However on the basis of information gathered it was ascertained that most of the employees involved in incidents that did not actually cause the organization any monetary loss, were not severely dealt with.

Where the employees caused monetary damage to the organization, the action ranged from severe reprimand to termination of employment.

The fact that 8% of the attacks were attributable to script kiddies is disturbing as in such incidents persons with relatively low knowledge are able to penetrate organizational networks using freely available "hacking tools".

The statistics are illustrated as under:



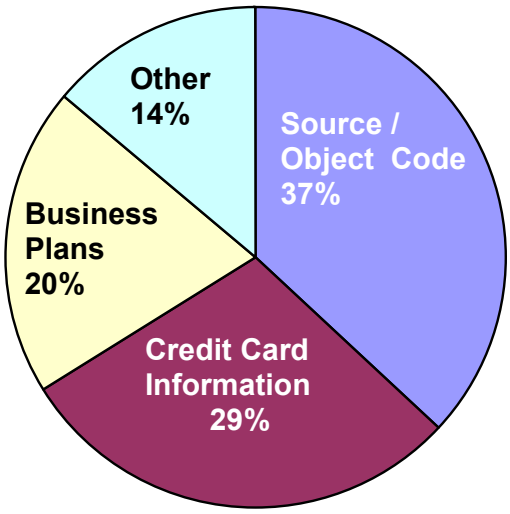
# DATA THEFT

This category accounted for 33% of the total reported incidents and includes theft and misappropriation of electronic information and records. Incidents of unauthorized access wherein no data was suspected to have been stolen have not been included in this category.

The major categories of data reported misappropriated include source and object code (37%), credit card information belonging to the organization's employees and customers (29%), business related plans (20%) and other confidential information (14%).

Of these cases of data theft 66% incidents involved an employee or former employee.

The categories of data stolen are illustrated below:




The methods employed for data theft showed a wide diversity.

**Email spoofing** was used in 52% of the incidents involving data theft. Email addresses of trusted employees, vendors and others were spoofed in order to misappropriate data.

**None of the organizations that had fallen prey to email spoofing were using Public Key Infrastructure** or any other system of entity authentication for email communication.

The use of **malicious code** (including Trojans, ActiveX bombs, scripting languages, exploitation of Field Code vulnerability of MS Word) has been used in 21% of the incidents of data theft.

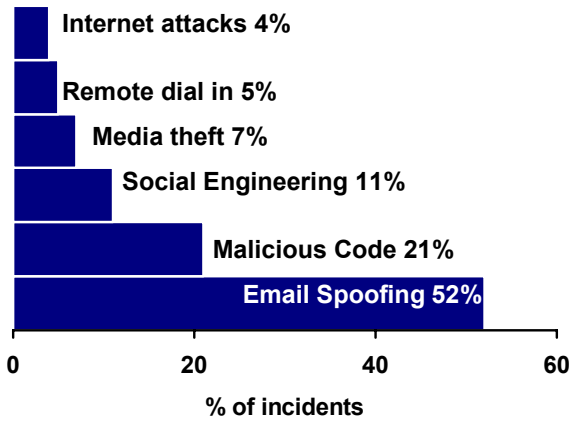
Social engineering techniques had been used in 11% of the incidents.

7% of the incidents involved media theft wherein laptops, computers, hard disks, removable media like floppy disks, CD ROMS etc were stolen.

5% of the data theft incidents involved the exploitation of remote dial in vulnerabilities while another 4% involved Internet based attacks (including primarily XSS attacks, SQL injection and cookie poisoning).

Although most organizations were not forthcoming in terms of the monetary damage caused by the data theft attacks, based on the responses of 40% of the victims of the data theft attacks, it is ascertained that the average cost of a data theft attack is Rs. 1.8 lakh.

The maximum loss disclosed was Rs. 1.87 crore while the minimum was Rs 20,000.



# EMAIL ABUSE

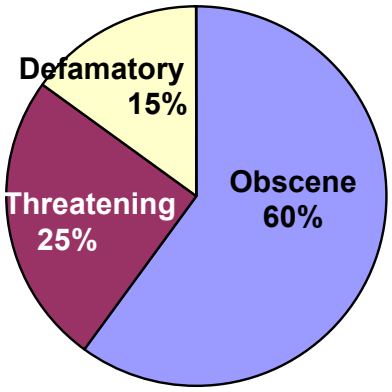
In this report, the term email abuse refers to incidents where the contents of the emails contained threatening, obscene or defamatory matter.

The term victim organization refers to the organization whose employees are the targets of the abusive emails.

60% of the incidents of email abuse related to obscene emails. Out of these obscene emails, almost all (97%) were sent to women employees.

25% of the incidents of email abuse related to threatening emails. Most of these were targeted towards the top management of the victim organization.

The balance incidents (15%) related to emails that sought to defame employees of the victim organization. The statistics are illustrated below:




An interesting trend in relation to email abuse incidents is that a vast majority of them (71%) are perpetrated by employees (or former employees) of the victim organization.

# DATA ALTERATION

Data alteration constitutes 14% of the incidents reported in 2001 and 17% of the incidents reported in 2002.

This category relates to incidents wherein unauthorized alteration of vital information takes place.

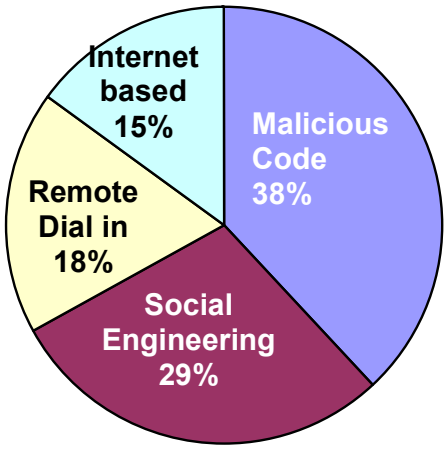
Incidents included alteration of hospital records, unauthorized changes made to quotations, financial accounts, bank records etc.

Although most of the incidents of data alteration involved unauthorized access, there were many instances where persons having authorized access to the data made the unauthorized alteration.

# UNAUTHORIZED ACCESS

This category, which accounted for approximately 19% of the total incidents, includes only those cases of unauthorized access wherein no data was suspected to have been misappropriated or stolen.

The methods employed for unauthorized access varied from use of malicious code (38%), social engineering (29%), exploiting remote dial in vulnerabilities (18%) and Internet based attacks (15%).




55% of the unauthorized access was traced to persons / departments within the organization, whereas 30% was traced to rival organizations while 15% was untraceable.

# VIRUS

This category refers only to those incidents where viruses were suspected to have been deliberately sent to the particular victim.

Incidents of virus attacks, where the victim organizations were affected by viruses that were "in the wild", i.e. unidentified and from the Internet, have not been included here. This report refers to cases of planned virus attacks targeted towards specific victims.

Although, this category reflects only 5% of the total incidents reported, it is significant because of the damage potential.

A sustained and targeted virus attack firstly can cause severe damage to the victim's assets and information.

Secondly, because the victim organization would unwittingly send out copies of the computer virus, it would be liable to pay compensation in crores of rupees under the Indian law.

These viruses were of various types including Stealth, Polymorphic, Companion, Armoured, and Macro viruses.

# DENIAL OF SERVICE

These attacks include denial of service attacks on web servers, mail servers, ftp servers and even printers!

This category accounts for 3% of the total incidents reported. The most interesting fact about this category is that most of the perpetrators were untraceable.

In 95% of the cases, the attack appeared to generate from outside India (mainly from USA and Pakistan).

The probability of IP spoofing, to mislead the victim about the location of the perpetrator, cannot be ruled out.

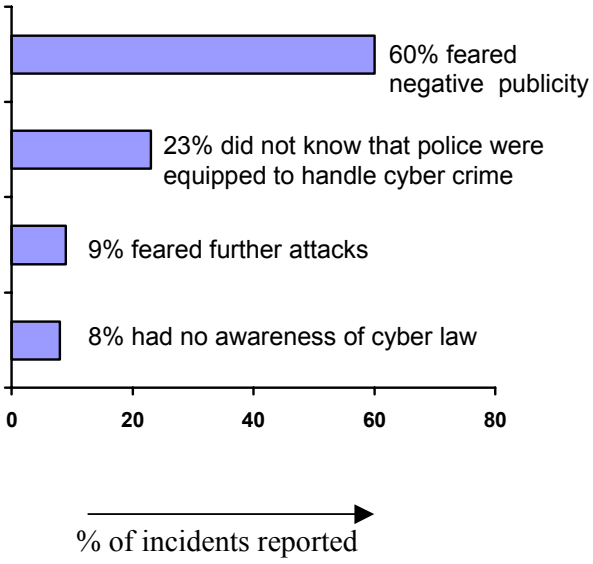
# REASONS FOR NOT REPORTING TO AUTHORITIES

Since this report covers only those incidents that have not been reported to the law enforcement agencies, the reasons for this non-reporting have been analyzed.

Over 60% of the victims did not report the incidents because of the fear of negative publicity. 23% did not know whether the police in their area were technically equipped to handle computer crime cases.

9% of the victims feared that if the incidents were reported and subsequently publicized in the media, then more such attacks would ensue.

8% of the victims did not know that Indian laws extended to computer crime. Most of these persons were under the impression that the Information Technology Act, 2000 was still a bill and consequently that there were no laws in India to cover computer crime and abuse.



# CONCLUSIONS & RECOMMENDATIONS

**Use of PKI is strongly recommended**

Incidents of data thefts, unauthorized access, and unauthorized data alteration can be eliminated by proper use of Public Key Infrastructure. This translates into the fact that 67% of computer crimes affecting corporates can be mitigated by proper implementation of inter and intra organizational PKI.

PKI is the super-system that puts in place policies, people, processes and technology to harness the power of cryptography and its applications like digital signatures.

The Indian law specifically recognizes digital signatures as being the only accepted mode of authentication of electronic records.

Although India is amongst the first few countries in the world to have granted legal recognition to PKI, its use remains minimal primarily because of the lack of awareness about its benefits.

A PKI based system would help in achieving the objectives of information security namely Privacy, Data integrity, Entity authentication, Entity identification, Message authentication, Signature, Authorization, Validation, Access control, Certification, Time stamping, Witnessing, Receipt, Confirmation, Ownership, Anonymity, Non-repudiation, and Revocation.

It is strongly recommended that organizations deploy PKI based systems.

The use of other cryptography based applications like secure socket layer etc are also strongly recommended.

**Incidents must be reported to the authorities**

The number of computer crime and abuse incidents that are not reported to the law enforcement authorities are staggering.

The passage of the Information Technology Act, 2000 followed by the subsequent amendment to the Indian Penal Code and the Evidence Act, amongst other laws, have paved the way for stringent penalties for computer crimes.

The Indian law provides for imprisonment up to 10 years and damages in crores of rupees for various computer crimes.

Moreover the law enforcement agencies in various parts of India are fast gearing up to tackle computer crime.

This is evidenced by the formation of cyber crime investigation cells in various cities and specifically the Cyber Crime Police Station at Bangalore, Karnataka.

The police and other law enforcement agencies in various states like Karnataka, Goa, Maharashtra, Gujarat, West Bengal, Delhi, Tamil Nadu, Andhra Pradesh etc have already displayed their skill in nabbing high technology criminals.

In such a scenario it is strongly recommended that organizations, and individuals, must immediately report any incident of computer crime and abuse to the local law enforcement authorities.

This would ensure that the guilty do not go scot-free and that a deterrent is created for others who dare to commit computer crime and abuse.

# LEGAL ISSUES

**Data Theft**

Although there is no specific legal provision that covers data theft, usually the theft of electronic data results in the diminishing of its value.

Under such circumstances data theft would be covered under Section 66 of the Information Technology Act, 2000 (IT Act), which recommends a punishment of upto three years imprisonment and / or fine upto Rs. 2 lakh.

The theft of source or object code is also included under data theft. The specific provision dealing with this is Section 65 of the IT Act.

A crime under this section is punishable with imprisonment up to three years and / or with fine, which may extend up to two lakh rupees.

**Email Abuse**

Sending pornographic or obscene emails are punishable under Section 67 of the IT Act.

An offence under this section is punishable on first conviction with imprisonment for a term, which may extend to five years and with fine, which may extend to one lakh rupees.

In the event of a second or subsequent conviction the recommended punishment is imprisonment for a term, which may extend to ten years and also with fine which may extend to two lakh rupees.

Emails that are defamatory in nature are punishable under Section 500 of the Indian Penal Code (IPC), which recommends an imprisonment of upto two years or a fine or both.

Threatening emails are punishable under the provisions of the IPC pertaining to criminal intimidation, insult and annoyance (Chapter XXII).

**Data Alteration**

Section 66 of the IT Act covers unauthorized alteration of data.

This section deals with hacking. According to this section, unauthorized alteration of data is punishable with three years imprisonment and / or fine upto Rs. 2 lakh.

**Unauthorized Access**

Unauthorized access is covered by Section 43 of IT Act, which provides for a penalty of upto Rs. 1 crore for this offence.

**Virus & malicious code**

Introduction of a computer virus or contaminant (including worms, Trojans etc) is covered by Section 43 of IT Act, which provides for a compensation of upto Rs. 1 crore for this offence.

If pursuant to the introduction of this malicious code loss of data occurs then Section 66 of the IT Act will also be applicable.

**Denial of Service**

This category has been dealt with under Section 43 of the IT Act, which provides for a compensation of upto Rs. 1 crore for this offence.

**Email spoofing**

Email spoofing is covered under provisions of the IPC relating to forgery (Chapter XVIII).

# IMPORTANT TERMS

**Computer Contaminant**

As per Section 43 of the IT Act, computer contaminant means any set of computer instructions that are designed to modify, destroy, record, transmit data or programme residing within a computer, or by any means to usurp the normal operation of the computer, computer system, or computer network.

**Computer Virus**

As per Section 43 of the IT Act, 2000, computer virus means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource

**Stealth virus**

A stealth virus is one that hides the modifications it has made in the file or boot record, usually by monitoring the system functions used by programs to read files or physical blocks from storage media, and forging the results of such system functions so that programs which try to read these areas see the original uninfected form of the file instead of the actual infected form.

Thus the viral modifications go undetected by anti-viral programs. However, in order to do this, the virus must be resident in memory when the anti-viral program is executed.

**Polymorphic virus**

A polymorphic virus is one that produces varied (yet fully operational) copies of itself, in the hope that virus scanners will not be able to detect all instances of the virus.

**Companion virus**

A companion virus is one that, instead of modifying an existing file, creates a new program, which (unknown to the user) gets executed by the command-line interpreter instead of the intended program. (On exit, the new program executes the original program so things will appear normal.)

This is done by creating an infected .COM file with the same name as an existing .EXE file. Note that this type of malicious code is not always considered to be a virus, since it does not modify existing files.

**Armored virus**

An armored virus is one that uses special tricks to make the tracing, disassembling and understanding of its code more difficult.

**Macro virus**

Many applications allow you to create macros. A macro is a series of commands to perform an application-specific task. Those commands can be stored as a series of keystrokes, or in a special macro language.

A macro virus is a virus that propagates through only one type of program, usually either Microsoft Word or Microsoft Excel.

It can do this because these types of programs contain auto open macros, which automatically run when you open a document or a spreadsheet.

Along with infecting auto open macros, the macro virus infects the global macro template, which is executed anytime you run the program. Thus, once your global macro template is infected, any file you open after that becomes infected and the virus spreads.

**Email spoofing**

A spoofed email is one that appears to originate from one source but actually has been sent from another source.

**Computer Source Code**

As per Section 65 of the IT Act, computer source code means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

**Unauthorized Access**

As per Section 2(1)(a) of the IT Act, access is defined as gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network.

Unauthorised access would therefore mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network.

**Denial of Service attack**

This involves flooding a computer resource with more requests than it can handle. This causes the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource.

**XSS attack**

An XSS attack (sometimes called cross scripting) occurs when an attacker uses a Web application to send malicious code, usually JavaScript, to a different end user.

**Social Engineering**

This refers to exploitation of personal relations with a person to obtain confidential information under his / her control.

**SQL Injection**

This primarily refers to attacks on websites which allow users to input data.

A user can exploit weak coding on the website to input malicious code, which then runs on the server or on the computers of other users.

An effective counter-measure is script validation wherein all data input by the user is sanitized. This ensures that the user can only send expected values, and not malicious script.

**Cookie Poisoning**

Cookie poisoning is a technique mainly used for achieving impersonation and breach of privacy through manipulation of session cookies, which are primarily used to maintain the identity of the user.

**Web-defacement**

The term “deface” means to “spoil appearance or beauty of, disfigure; make illegible”.

Web Defacement occurs when the attacker spoils the appearance of the website of the victim organization.

In most cases the perpetrator leaves obscene messages on the website.