NEED OF INFORMATION SECURITY IN THE 21ST CENTURY: WITH SPECIAL EMPHASIS TO COMPUTER SECURITY

Anjana Bhatnagar

Abstract

We are living in a society dominated by information technology and in an era of information where huge amount of Information can be speedily processed and saved on easily accessible media. Information plays a really important part in decision making in an organization. For an organization a wrong decision can lead to drastic result. This is on reason why information is steadily acquiring a more central role in business. In the world of today information is becoming increasing important. Generally speaking the standard of information security has not kept pace with this development. For example, information that before was saved on a large amount of paper and physically difficult to steal can today be saved on a disk that can easily remove.

In this article author has discussed, what information security is. Why it is needed in an organization of 21 century. The CIA Relationship of information security is discussed with diagram. The information security chain has twelve modules and eighty sub modules. The overview of information security cannot be complete in such small paper; therefore author delimits herself to the most prominent module computer security. In the last future and conclusion of information security are highlighted. Information Security of IIT Kanpur system is also consulted in some of the modules. The paper is of particular value for newcomers in this area.

Keywords : Information Security, Computer Security, Computer Viruses, Data Encryption, Biometric Methods

1. Introduction

Information security deals with several different 'trust' aspects of information. Another common term is information assurance. Information security is not confined to computer systems, nor to information in an electronic or machine-readable form. It applies to all aspects of safeguarding or protecting information or data, in whatever form. Information security chain is needed when information is threatened, lost or misused.

2. Methodology

The paper is aimed at presenting the need of information security in 21st century. The Data for this paper is based on conceptual study including personal observation and interaction with students, faculty, staff involved in it and library research referring to the important journals, periodicals, publications and research volumes and making use of the web to build up first hand information for future analysis. Data display involves organizing and assembling reduced data into diagrammatic or visual display.

3. Scope of the Information Security

Information security is a protection of the interests of those relying information and the information systems and communications that deliver the information from harm resulting from failures of availability, confidentiality, and integrity. [1]

The organization's information security policy aims to ensure that:

- its information systems are properly assessed for security
- confidentiality, integrity and availability (CIA) are maintained. These three concepts are at the core of almost every security program–if not by name, at least in practice. They are most commonly described as a triangular view of security, with each side directly related to the other two. As shown in Figure1. **Confidentiality** – information access is confined to those with specified, explicit authority to view the information. **Integrity** – safeguarding the accuracy and completeness of information. **Availability** – ensuring that authorized users have access to information when needed.
- staff are aware of their responsibilities, roles and accountability
- procedures to detect and resolve security breaches are in place
- information security issues are dealt with consistently throughout the organization

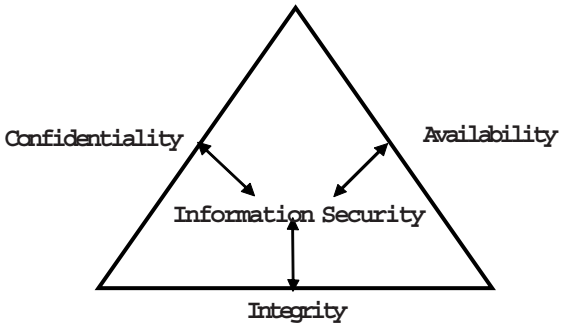


Figure 1: The CIA Relationship

4. What Is Information Security ?

We are a part of an information Society. Huge amount of Information can be speedily processed and saved on easily accessible media. Information plays a really important part in decision making in an organization. For an organization a wrong decision can lead to drastic result. This is on reason why information is steadily acquiring a more central role in business. In the world of today information is becoming increasing important. Generally speaking the standard of information security has not kept pace with this development. For example, information that before was saved on a large amount of paper and physically difficult to steal can today be saved on a disk that can easily be removed. Information security is an attempt to protect information by making it accessible only to the intended individuals groups or organizations. The reason may be financial, political, tactical or purely logistical. Every organization depending upon its resources, and the type of data it handles, has allowed a separate budget and manpower for developing information security arrangements.

According to Dr. Thomas V. Finne [2] information security chain has twelve modules and eighty sub modules as below:

4.1 Computer Security : This module includes seventeen submodules - Backup, Computer Viruses, Passwords, Data Encryption, Biometric Methods, Off-site Storage, System Backup, Cold and Hot Sites, Card Access, Disk-Free Station, Computer Locks, Printer and Fax Security, Diskette Security, Rescue Diskette, Distributed Systems, Outsourcing, Time Sharing and Remote Office, Log Functions, Locked Hardware.

4.2 Operation Security: Software Security, Illegal use of Software, Spread sheeting and DSSs, Data Input Security, Data File Destruction, Data Compression, Utility Programs, System Administration, Data Leakage, Super zapping, Entrapment, Database.

4.3 Protection against Burglary: Security Guards, Alarms, Access Control, Safes.

4.4 Protection against Fire: Alarms, Sprinklers, Fireproof Safes and Cupboards.

4.5 Protection against Water Damage: Building Materials and Construction, Water Sensors, Flooding.

4.6 Electricity Distribution: The Electricity Supply, Allergy to Electricity, Magnetic Fields, Electromagnetic Fields.

4.7 External and Internal Threats: Sabotage, Espionage, Abuse, Public Information.

4.8 Communication: Telephone Lines, Cable Security, External Contact, Dial-up, Firewalls, Mobile Computing.

4.9 Contingency Planning: Emergency, Recovery.

4.10 Personnel Security: Recruiting, Control of Personnel, Access to Information, Human Mistake, Contract Employees and Visitors, Unauthorized Work, Staff Shortage, Theft by Staff, Impersonation, Piggybacking, Officer Appointed to be Responsible for ISEC, ISEC Education, Incident Reporting.

4.11 Attitudes toward ISEC Issues: Written Security Policy, Information Security Culture.

4.12 Various Security Questions: Atmospheric Humidity, Document Security, Temperature, Dust, Smoke, and Particles, Optical Spying, the Environment, Tailgating, Scavenging, Shoulder Surfing, Building, Mail Security.

5. Computer Security

Computer security measures, procedures, and controls which provide an acceptable degree of safety of information resources from accidental or intentional disclosure, modification, or destruction. Sub modules of computer security are as below.

5.1 Backup

Backup means having multiple copies of the same data so that the duplicate ones can be used in case the original one gets corrupted or erased accidentally. Though having backups may seem as a waste of time but they often come in handy when one actually needs them. [3] Backups must also be tested so as to avoid failure owing to human or machine malfunctioning. Of the different media that can be used for doing backups it is important to have effective, reliable and user friendly backup software. Instead of having a backup of all the files, it is advised to have it for just the most important ones. Backup in IIT- Kanpur - User home directories on the central file server are backed-up on daily basis. The daily incremental backup is taken and kept for a week. On first Sunday of every calendar month, all files are saved on tapes. This backup is retained for one year. On other Sundays of the month a weekly backup is taken which is retained for a month. From Monday to Saturday, incremental backup is taken which is recycled in the next week. [4] Computer Centre operates 24 hours a day, 365 days an year. It has a power back up through a 180 KVA UPS and a 320 KVA generator set. Air conditioning is provided by the central air conditioning plant and split air conditioners.

5.2 Computer Viruses

Viruses are defined as 'A section of code introduced into a program for malicious purposes, e.g. at some stage the inserted code will trigger a process which will, for example, eliminate files. The virus is present in a program, and when the program is run the virus writes itself into other programs in main memory or backing store. The effects of virus can thus be extended to many users'. [5] There are many kinds of computer viruses like Worms, Bombs, Trojan horses and Computer viruses. A way to avoid computer viruses is always to test the software before installing it and to avoid pirated software. Viruses can be spread through emails also. Some of the most well known viruses are Bugbear, Klez, Lovebug, Melissa, Bubbleboy, Code Red, Nimda. There are six recognized categories of virus as below:

Boot Sector Virus: Replaces or implants itself in the boot sector—an area of the hard drive (or any other disk) accessed when you first turn on your computer. This kind of virus can prevent you from being able to boot your hard disk. Eg. Disk Killer, Michelangelo, stoned
File Virus: Infects applications. These executables then spread the virus by infecting associated documents and other applications whenever they're opened or run. Eg. Jerusalem and Cascade
Macro Virus: Written using a simplified macro programming language, these viruses affect Microsoft Office applications, such as Word and Excel, and account for about 75 percent of viruses found in the wild. A document infected with a macro virus generally modifies a pre-existing, commonly used command (such as Save) to trigger its payload upon execution of that command. Eg. W97M.Melissa, WM.NiceDay, W97M.Groov
Multipartite Virus: Infects both files and the boot sector—a double whammy that can re- infect your system dozens of times before it's caught. Eg. One_Half, Emperor, Anthrax, Tequilla.
Polymorphic Virus: Changes code whenever it passes to another machine; in theory these viruses should be more difficult for antivirus scanners to detect, but in practice they're usually not that well written.
Stealth Virus: Hides its presence by making an infected file, not appear infected, but doesn't usually stand up to antivirus software.

5.2.1 Worm

A worm is a program that is designed to replicate and spread throughout a computer system. It will usually hide within files (for example, Word documents), and distribute those files through any available network connections. Worms are often used to drain computer resources such as memory and network access, simply by replicating on a large scale. Eg. W32.Mydoom.Ax@mm

5.2.2 Trojan Horse

A Trojan horse is a malicious program, usually disguised as something useful or desirable. When activated, they can cause loss, damage or even theft of data. The critical difference between a Trojan horse and a virus is that a Trojan horse cannot replicate itself. The only way that a Trojan horse can spread is if someone helps it. Trojan.Vundo is a Trojan. For example, saving the program from an e-mail attachment, or downloading it from the Internet. Some common features of Trojan horse programs include:

- Rounding (carving off small parts of payments from a large number of accounts or transactions),
- Causing payment triggers (causing illicit payments to be activated),
- Making configuration changes,
- Distributing security information, providing unauthorized access paths (known as backdoors and trapdoors).

5.2.3 Precautions

Protection against Computer Viruses, Worms and Trojans are :

- Run anti virus software recommended from the information security division of organization and make sure that version should be current and latest.
- Don't open macros attach files from unknown email. Delete these attachments immediately.
- Delete spam, chain, and other junk email without forwarding.
- Don't download files or email attachments from unknown or unauthorized sources.
- Scan a floppy diskette from an unknown source for viruses before using it.

New viruses are discovered almost every day. Up-dation of anti-virus software should be done only through designated sources, and do not trust any other sources for virus protection patches. The list of latest virus threats can be seen from the Table 1. [6]

It provides a synopsis of the latest virus-related threats discovered by Symantec Security Response, including information on Category Rating (risk), Name of Threat (threat), the day on which the threat was identified (discovered), and the day on which a virus definition was added to protect against the threat (protection). Click on the name of the threat for additional information. If the threat in question is not recent, it may still be located via Symantec Security Response from this.

Name	Detected	Protected
Trojan.Advatrix	10/25/2007	10/25/2007
Trojan.Sushpy	10/24/2007	10/24/2007
Trojan.Nssearch	10/23/2007	10/23/2007
Bloodhound.Exploit.163	10/23/2007	10/24/2007
W32.Usbwatch	10/23/2007	10/23/2007

Table 1: List of Latest Viruses Threat

5.3 Passwords

These play significant role in computer security. Passwords should be complicated and should contain both numbers and letters. The passwords should not have user's name, license plates etc. but some imagination should be used. Every computer user in an organization has to observe good password security. Their password security can be checked, however because once a user selects a password, the system administrator can use a password checker to automatically check if the password

is suitable. In a company where there are several servers and networks in use, user has to remember many passwords. In this case the user tends to use similar passwords for different systems, which in turn increases the security risk. Thus to avoid this access control packages that includes passwords, logs, encryption and so forth must be used. By using such packages it can be possible to avoid using many password systems. Vendor supplied passwords should be changed immediately. IIT Kanpur Computer Centre provides login and passwords to the faculty, staff and students for their research and teaching. It has a users base of more than 6000+ users with more than 1000 active users at any given point of time.

5.4 Data Encryption

Data encryption is a means of securing data by changing the meaningful text into some code which looks like null and void to others. It's a reasonably easy way to protect information. The user has to remember the key and the software and hardware is secure and user friendly. According to Hoffman there are 900 cryptography hardware and software products on the market. [7]

The System administrator normally has access to all files in an information system, therefore the administrator can be a great information security risk, and the risk can be minimized, however, if the classified files are encrypted. The administrators still do his work. [8]

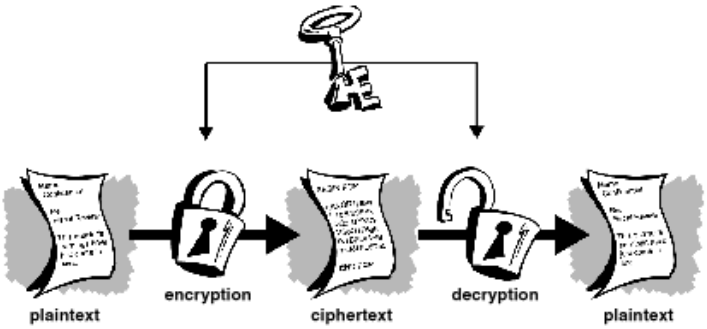
5.4.1 How does Encryption Work?

Encryption involves taking an original message or plaintext and converting it into cipher text (unreadable format) using an encryption algorithm and an encryption key. Only those who posses a secret key can decipher the message into plain text. Historically, encryption acted on letters of the alphabet. The Caesar Cipher, one of the oldest techniques, gives a very simple example:

- Take the plaintext is Parliament is in session;
- Encrypt according to the encryption algorithm 'replace each letter with that X places to the right of it in the alphabet', where X, the encryption key, is 3;
- The cipher text is sduoldphqw lv lq vhvvlrq and can be converted back to plaintext with a decryption algorithm and decryption key, in this case 'replace each letter with that three places to the left of it in the alphabet'.

Computers store electronic data in binary form, as sequences of 'bits' (1s and 0s). Modern algorithms are mathematical functions that act on these data with keys that are themselves sequences of 1s and 0s. Keys are generally stored in computer files that are themselves encrypted and can be accessed only with a pass phrase (similar to a password but longer). We can see its working Figure 2. Encrypted messages can sometimes be broken by cryptanalysis (coding breaking) but modern

cryptography techniques are virtually unbreakable, eg. Cryptography is to protect- email messages, credit card. Most popular systems used on the internet are Pretty Good Privacy because it is effective and free. [9]



5.5 Biometric Methods

Biometric methods include those of voice, face, hand geometry, fingerprints, eye, signature and typing rhythms as shown in Figure 3. When combined with good password security, can give high information security but it need high cost biometric instruments.

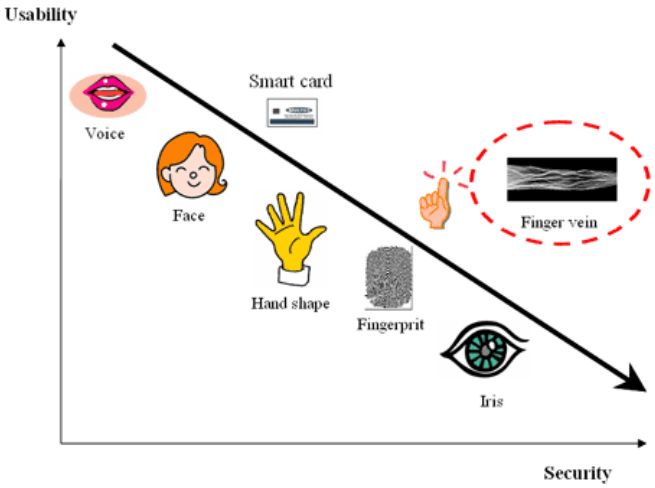


Figure 3: Examples of Biometric Methods

5.6 Off-Site Storage

Off-site storage means storing the backup files in a secure place. They should preferably be encrypted. So many commercial organizations are available in the market in specializing in storing

'organization backup'. So there is no need to build its own storage facilities. The organization storing the backups has to be extremely reliable.

5.7.1 System Backup

Most organizations think that system backups (backup of networks) are unnecessary because the software is easily available from the distributors. On the contrary it is a nice practice to have spare systems which are tested regularly.

5.8 Cold and Hot Sites

Cold sites are empty computer rooms with everything besides computers and communications systems installed. [10] For example, in case of emergency (fire, earthquakes etc,) computer centre destroyed, it can be useful to have a cold site. Hot sites on the other hand are fully equipped "spare" computer centers. These are recommended for organizations with an extremely heavy reliance on computers. Spare computer centre can be approximately 50 percent of the capacity of the original one. Both hot and cold sited can be shared by many organizations.

5.9 Card Access

Using plastic cards for accessing PCs can improve information security in an organization. It is usually combined with the use of a personal code. Cards can be provided with the photograph of the user too. A log in a microcomputer can register when a card is used. To avoid unauthorized use of a card, lost cards have to be blocked immediately.

5.10 Disk-free Stations

Use of disk-free stations and passwords to access the server can minimize information security problems in an organization where there are hundreds of PCs connected in a network. By this only a few key persons will have authorization to copy information on to diskettes.

5.11 Computer Locks

Servers should be provided with a computer lock in its disk station. The key to the computer should be kept safe and must not be lost. The PCs are provided with an inbuilt lock that can be used to shut them off.

5.12 Printer and Fax Security

Printers should not be provided with terminals if it is possible to take printouts of classified material. [11] Printers should be kept in locks. In an organization it is common that many people share a printer. This means that the material printed out can be seen by many people and if the printer is not kept behind locked doors. There can be considerable damage. Another considerable problem with

faxes is that the sender can easily dial the wrong number by mistake. Managers should have their own fax machine. This naturally implies that the managers are reliable enough and they do not use the fax for sending out sending out documents to a competitor.

5.13 Diskette Security

A diskette containing, important information should not be sent my mail. Such a procedure should be avoided since the diskette can be stolen, copied, or damaged during transportation. Electronic data interchange should be used. Diskettes are stored in properly in a safe place and in an organized manner.

5.14 Rescue Diskette

rescue diskette should include the most important utilities, in the case of a PC, especially the .com, .dat, .exe, .ini and .sys files. The rescue disk can be very useful, when a user is attacked by computer viruses. The rescue diskette has to be properly stored.

5.15 Distributed Systems, Outsourcing, Time Sharing and Remote Office

Distributed systems, outsourcing, time sharing and remote office fairly new processes in IT bring new information security concepts. **Distributed system** means moving from traditional large computers to open client / server systems. In distributed environment every employee's responsibility for information security increases. **Time sharing** means that organizations share computing services and in that way decrease costs. Risk increase in this. The resources saved by using shared premises and **outsourcing** can easily be lost in an information security break. Those involves have to be extremely reliable. **Remote office** means carrying out the work at home or at another location by means of modern telecommunication. Data transmission should be encrypted. Information security must not hinder an organization from carrying out a remote office operation, but the questions for information security have to be observed.

5.16 Log Functions

A log function registers when a PC was used. By using a log it is possible to determine, afterwards, if files have changed in order to commit a fraud.

5.17 Locked Hardware

Hardware should be locked, for example, office furniture etc. This makes it more difficult to steal the hardware. Thieves are interested in only Computers and especially hard disks.

6. Conclusion

Information security is the ongoing process of exercising due care and due diligence to protect information, and information systems, from unauthorized access, use, disclosure, destruction, modification, or

disruption. The never ending process of information security involves all modeules of information security. The academic disciplines of information security and information assurance emerged along with numerous professional organizations during the later years of the 20th century and early years of the 21st century. The profession of information security chain has seen an increased demand for security professionals who are experienced in network security auditing, penetration testing, and digital forensics investigation. The Prabhu Goel Research Centre for Computer and Internet Security at IIT Kanpur was established by Dr. Prabhu Goel in 2003. The vision of the centre is to become the nodal R&D centre in the country for all aspects of computer security and to educate various governmental and non-governmental organizations on the security issues and help them in this regard. The centre is therefore undertaking research, training, and consulting activities in the area of computer and Internet security. The centre also collaborates with defense and security agencies in developing various security technologies. IIT Kanpur has already been doing work in the area of Computer Security. The establishment of this centre is expected to give a tremendous fillip to this activity.

Biometric methods will grow in popularity as the price of biometric instruments declines and their operational security increases. Cryptographic methods remain the most obvious tool for information security. As hardware gets faster, the processing load for encryption and authenticating messages can be expected to decline. This is obviously true if the key length stays the same, and almost as certain if measured as the time it takes to encrypt a message which takes a fixed *X* hours decrypt (as supercomputers get better, the required key length rises). Thus, everything else being equal, cryptographic methods will see greater use, and information security will rise.

The profession of information security chain has seen an increased demand for security professionals who are experienced in network security audint, auditing, prenetration testing and digital forensics investigation. So to secure an organization there is a need of information security in 21st century organization.

References

1. (IFAC 1998. Exclusive Summary) Managing security of information of information technology committee, website at www.ifac.org/new]
2. Thomas V. Finne ; Encyclopedia of Library and Information Science By Allen Kent Marcel Dekker, New york V.65 p.p 139-166
3. J. Maynard, *Computer Audit Update*, UK, Dec.1994, pp 15-18
4. http://www.iitk.ac.in/cc/services.htm#login accessed October 27, 2007
5. W. Caelli, D. Longley and M. Shain, *Information Security for Mangers*, Stockton, Uk, 1989

6. http://www.symantec.com/business/security_response/threatexplorer/threats.jsp accessed on October 26, 2007
7. L. Hoffman, Encryption Policy for the Global Information Infrastructure, in *Information Security: the next Decade,* J. Eloff and S. Von Solms, ed. proceedings of the IFIPTC11 Eleventh International Conference on Information Security, South Africa, May 9-12, 1995, pp 50-63]
8. LAN Vision Oy, Tietoturvauutiset, no 1, 1995, p.4
9. http://www.pgpi.org/doc/pgpintro/ accessed on October 26, 2007
10. C.C.Wood, *Effective Information Security Management*, Elsevier Advanced Technology, Oxford, UK, 1991
11. M. Smith, Commonsense Computer Security; your practical guide to information security. McGraw Hill, London, 1993.

Work cited

- http://computer.howstuffworks.com/encryption1.htm accessed on October 26, 2007
- http://www.pbs.org/newshour/science/computer_worms/works.html accessed on October 26, 2007

ABOUT AUTHOR

Dr. Anjana Bhatnagar is working in PK Kelkar Library at IIT-Kanpur since 1983. She has made significance contributions towards Library Software development, iit-KLAS running successfully at IIT Kanpur. She is also one of the member in developing Library Software 'SoftGranth', the modified version of iit-KLAS.