Information Systems: its Security and Control

A. Sravani

Associate Professor, Department of

Business Management, Sarojini Naidu

Vanita Maha Vidyalaya, Exhibition

Grounds,Nampally, Hyderabad – 01

Email: sravani_vms@yahoo.co.in

****

Abstract

Data transformed to the Information and now the talk is of its Security. In the present world, the flow of information and its storage has begun an important task for every individual, organisation and also to the government. The security means protecting the information from an unauthorised access and use. The Information security is also concerned with the identification of an organization's electronic information assets and the development. It is also concerned with that of the execution of tools and techniques, policies and procedures, standards and guidelines and so on, to ensure the confidentiality, integrity and availability of these assets.

Keywords: Information, Security, Malicious Software and Information System control.

Introduction:

Inclusion of global internet and the information system and their infusion into the operations and management of businesses, government organizations, and also into the infrastructure, information security issues have moved to ahead of concerns about global well-being.

What Is Security?

In general, security is something that is not likely to fail or be lost". In other words, protection against those who would do harm, intentionally or otherwise is aim. National security, a multilayered system, actually talks about the protection of sovereignty of a state, its assets and resources, and its people. In the same, security for an organization also requires a multifaceted system.

The National Institution of Standards and technology (NIST) defines Information Security based on the 44 United States Code System 3542 (b) (2), which states that an Information Security is protection of information and information systems from illegitimate opening and using, leaking the information and creating the trouble, modifying and ruining of the data to

provide integrity, confidentiality and availability of the data."

The following are the layers of security to protect the information of any successful organisation:

- Physical security: the protection of physical items, objects, or areas from unauthorized entrance and misuse
- Personnel security: the protection of the individual or of the group who have the authorization to access the organization and its operations related data or information.
- Operations security: protection of the organizational activities or operations.
- Communications security: protection of the communication content and technology and media
- Network security: protection of networking components, connections, and contents
- Information security: protection of information both inflow and outflow of the data

The Committee on National Security Systems (CNSS) defines the information security as the protection of information and its significant elements, together with the systems and hardware that are employed, stored, and transmitted information in any of the organisation.

Information Systems Security:

Information systems security is responsible for the integrity and safety of system resources and activities. Most organizations in developed countries are dependent on the secure operation of their information systems. In fact, structure of the societies often depends on this security. Several infrastructural networks, which include power, water supply, and health care etc, rely on it. Institutions cannot survive without the information systems.

A. Confidentiality:

Confidentiality of the information is to know about the one who is allowed to access the data or the information. In other words, preserving personal privacy is the main aim of the Confidentiality of the information. This actually prevents the unauthorized leakage of information and permits the data access to only authorized persons. The aim of making information accessible to many is becoming an obstacle to maintain the principle of confidentiality.

B. Integrity:

In any business organization having IS, the values of data stored and manipulated, such as maintaining the correct signs and symbols is an important issue of concern.

C. Availability:

The accessibility and the usable form of data and information when and where it is needed is known as Availability. That is the prevention of withholding of data or resources illegally.

1) System Vulnerability and Abuse

When data is stored in a digital form, they are more vulnerable at risk, than when they exist in manual form. In other words, there is more risk involved in the digital form of data, than the other. Information System Security refers to prevent not permitted access or change of the

information, theft or physical damage of the information systems using policies, procedures, and technical measures.

Information system Controls consist of the policies and procedures of safety of the organization's assets; accounting records; and maintenance of management standards.
Information system Threats include hardware and software failure; error and physical disasters, illegal use of data; and telecommunications disruptions. Information systems and telecommunications added to internet are especially vulnerable to threats because data files can be directly accessed through computer terminals.

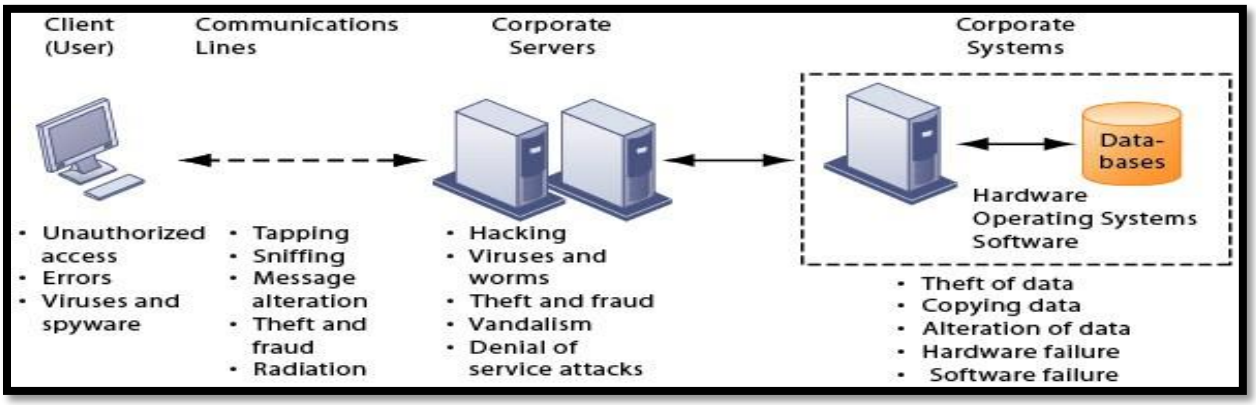

FIGURE.1: CONTEMPORARY SECURITY CHALLENGES AND VULNERABILITIES

The integration of organizational related information computer systems with that of the Internet to make the availability accessibility of the data and the information to people may add in many other problems like hacking of the data, introduction of new viruses and also malicious software etc.

And in the Wireless networks the radio frequency bands, which can be easily scanned will create more problems in sharing of the information. Local Area Networks (LANs) that use the Wi-Fi connections can easily be hacked by the hackers. Wired Equivalent Privacy (WEP), the security standard is not very useful. WEP is built into all standard products, which users must turn it on, but they don’t do and leave many access points unprotected.

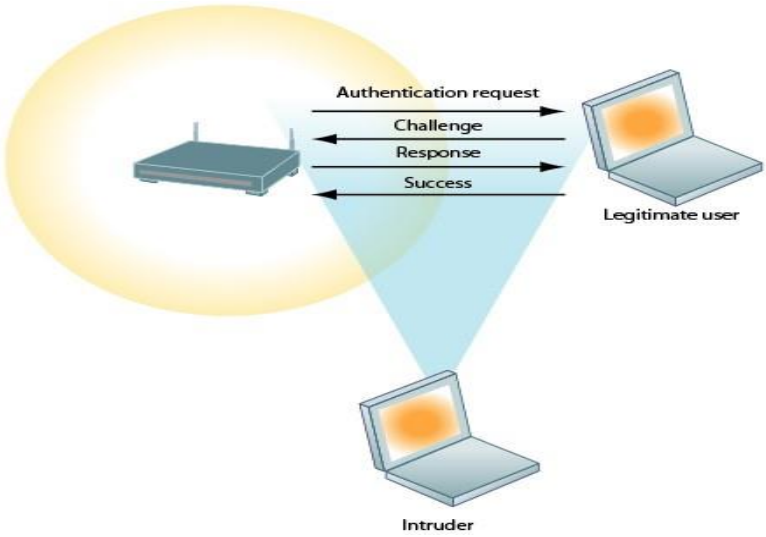

FIGURE 8-2: WI-FI SECURITY CHALLENGES

Malicious software, or malware, includes threats such as computer viruses and worms, and Trojan horses.

- A **computer virus** is software that attaches itself to other programs or data files in order to be executed, and may be highly destructive to files, computer memory, and hard drives. Viruses are typically designed to spread from computer to computer through e- mail attachments or copied files.
- **Worms** are independent computer programs that copy themselves to computers over a network independently from other computer programs or files, and therefore spread more rapidly.
- A **Trojan horse** is an apparently benign program that actually performs some hidden action such as installing malicious code or compromising the security of a computer.
- **Spyware** can also act as malicious software by obtaining information about users buying habits and infringing on privacy.
- **Key-loggers** record keystrokes made on a computer to discover steal serial numbers for software and passwords

A **'hacker'** is an individual who is an unauthorized person get the access to a computer system. These hackers actually take-off or misrepresent themselves, by using false e-mail addresses. Hacker activities includes as follows:

- **Theft of Goods and Services**
- **System damage**
- **Cyber vandalism:** The intentional trouble or damage of a Web site or organizational information system.
- **Spoofing:** Here the hacker may not show his or her true identities or email addresses. Or he or redirecting a Web link to a different web site that benefits the hacker.
- **Theft of proprietary information:** A sniffer is an eavesdropping program that

monitors network information and can enable hackers to steal proprietary information transmitting over the network.

- **Denial of Service (DoS) attacks:** Flooding a network or server with thousands of false communications to crash or disrupt the network. A distributed denial-of-service (DDoS) attack uses hundreds or even thousands of computers to inundate and overwhelm the network from numerous launch points. Hackers can infect thousands of unsuspecting users' computers with malicious software to form a Botnet of resources for launching a distributed denial-of-service (DDoS).

In computer crime, the computer can be either the target of or the instrument of a crime. The very different kinds of system crime related to computer world are DoS attacks, introducing viruses, theft of services, and trouble of computer systems.

Other examples of computer crime include are as follows:

- **Identity theft**: In identity theft, an impostor obtains key pieces of personal information to impersonate someone else and obtain credit, merchandise, or false credentials.
- **Phishing**: To obtain information such as usernames, passwords, and credit card details etc often for cruel reasons, by hiding the entity information in an electronic world.
- **Malicious Intruders:** The largest financial threats to businesses actually come from insiders, either through theft and hacking or through lack of knowledge. Malicious intruders may sometimes trick employees into revealing passwords and network access data through social engineering. Employees can also introduce faulty data or improperly process the data.
- **Software errors:** These are also a threat to information systems and cause untold losses in productivity. Hidden bugs are overlooked by programmers working while programming, can cause performance problems and security threats. Software vendors create lines of code called patches to repair flaws without disrupting the software's operation.

Seeing the above we can easily conclude that the information systems are at risk. This actually needs to be strictly controlled. The security of the information system may include continuous countermeasures and standard auditing process maintenance by the organisations. This also is the responsibility of the users to see and follow the secured devices and processes. A plan should also be made to cover the failure of servers, networks, software and others.

Information Systems Controls:

For the safety and security of the information systems and its efficient utilization, an organization institutes a set of procedures and measures called Information system controls. There are two types of Information systems controls. They are as follows:

a) **General controls** apply throughout an organization to the information system actions. These are the common measures that control the access to computer systems and the

information stored or transmitted over the networks. General controls also include managerial measures that restrict the internal employee's use and access of the computers; only to those processes directly relevant to their work have the accessing authority. Of which, these controls edge the harm that any internal employee will be doing to the system. In the case of the breakdown of the primary information system the backup systems may be activated.

b) **Application controls** are specific to a given purpose. These controls include measures as validating raw data, sorting the accesses to the computer system, regularly storing of the copies of various databases, and ensuring that the information is spread only to authorized users and organisations.

Securing Information:

Secured access of the information from the computer systems became greatly more difficult with the increase of the connection of Wide Area Networks (WANs). Users and others may access systems from any unattended computer using the internet services within an organization or outside. For security reasons, each legitimate individual will have a unique name and a password. And another security measure is the physical authentication, such as an object such as a physical token or a smart card or a personal characteristic like fingerprint, retinal pattern, hand geometry, or signature.

Many computer systems combine these types of measures. They are like Automatic Teller Machines (ATM), which depends on a Personal Identification Number (PIN) and a card. Also Firewalls helps the organisations to have buildup Security measures placed between an organization's networks and the Internet. These filter all the incoming and outgoing data.

Encryption is another way of security measure which prohibits the access to information, gained importance in electronic commerce. Public key encryption is used widely in electronic commerce to ensure confidentiality. And only the planned receiver has the private key, which is needed to decrypt the information or the messages received by him that have been encrypted with the receivers public key.

Furthermore, authentication of both parties is through the digital certificates which are issued to both parties by a trusted third party and the use of digital signatures, which is an additional code attached to the message to verify its originality. To detect fraud, a kind of anti-tampering code will also be attached to get the message. Similar means are available to ensure that the people involved in an electronic transaction cannot later deny their contribution.

For continuous monitoring the information systems, interference discovery systems are used, which detect irregular events and register the information necessary to create reports. This also helps to establish the basis and the kind of the possible interruption happened. More active are the computer systems the effort to check the interruption or the detection of the fraud happened will be easy.

References:

1) Kenneth C. Laudon & Jane P. Laudon, "Management Information Systems: Managing the Digital Firm", Pearson Education. http://paginas.fe.up.pt/~als/mis10e/ch8/chpt8-1bullettext.html
2) Anita Goel, "Computer Fundamental", Pearson Education.
3) Turban, Rainer, & Potter, "Introduction to information Technology", Wiley India.
4) Abraham Silberschatz & Peter Baer Galvin, "Operating System Concepts", John Wiley & sons.
5) www.britannica.com/topic/information-system/Information-systems-audit#toc218075
6) http://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf
7) https://bus206.pressbooks.com/chapter/chapter-6-information-systems-security/
8) www.sans.org/information-security/