

FESTUS OLUBUKUNMI AJIBUWA
ID UB3241SCS7932

School of Science and Engineering

DATA SECURITY

Submitted as partial fulfillment of academic requirements for:

ATLANTIC INTERNATIONAL UNIVERSITY

Introduction

Security according to Collins English Dictionary is “the state of being secure. Precautions taken to ensure against theft, espionage, etc;” Data security is very important, data that contain personal information has to be protected under the data protection act, and data that could be useful for commercial competitors has to be safeguarded from theft.

The Higher National Computing (page 226) declares that data security as an essential aspect of computing especially with database system to ensure privacy of sensitive and personal information. Data security is also paramount in complying with legislation that protects users and third parties of data.

A number of organizational security breaches can occur; some of these are amplified by the use of a database because of the integrated approach to data storage and retrieval. Some of these breaches and security issues include:

- Virus
- Unauthorized access (hacking)
- Industrial and/or individual sabotage
- Accidents by users (incompetence)

According to Terence Driscoll and Bob Dolden “Security in information management terms means the protection of data from accident or deliberate threats which might cause unauthorized modification, disclosure or destruction of data, and the protection of information system from the degradation or non availability of services.”

Security refers to technical issues related to the computer system, psychological and behavioral factors in the organization and its employees, and protection against the unpredictable occurrences of the natural world.

Kelvin Townsend (editor, Information Security Bulletin) mentioned on page 10 of the IMIS IT Security journal that people frequently asked him “What is the best security system to install?” And his answer is “The best security system is the one that allows you to fulfill your security policy.” He further said that “A formal security policy is the key to a secure system.”

And in his analysis of some of the threats and risks to data, he mentioned the following:

Loss of access to your company data

Unproductive workforce

Viral infection

Theft of company secrets

Inadvertent law breaking

Security can be divided into a number of aspects:

- (a) Prevention
- (b) Detection

- (c) Deterrence
- (d) Recovery procedures
- (e) Correction procedures
- (f) Threat avoidance.

Crimes and instructions on automated information systems

Computer crime encompasses any unauthorized use of a computer system including software piracy or theft of system resources for personal use including computer processing time and network access time. It is also a crime to take any action intended to alter data programs or to damage or destroy data, software, or equipment. All these crimes are committed through intrusion, the forced and unauthorized entry into a system.

Computer crime through intrusion can occur in one of two ways, which is either by hackers break into a system to destroy the data or the network, or software viruses inserted into a system to destroy programs and data.

Software Piracy

Piracy is the act of making of illegal copies of copyright information, and software piracy is the making of illegal copies of software. This is one of the most serious issues in IT today because it is so widespread that it is responsible for an enormous loss of revenue to software originators.

Protections against Software Piracy

Software Copyright Protection: This is the legal protection of original works against unauthorized use, including duplication, provided the owner visibly displays a notice on the product. This method has been used for many yeas for the protection of books, magazines, music and other commercial original works, but today it also applies to computer software, database etc.

Copyright Protection: This is a software protection scheme that defeats attempts to copy a program or makes the copied software unreliable.

Software Site Licensing: This is an agreement under which a software purchaser pays a fee to the manufacturer to make a specified number of copies of a particular program.

Hackers

Hackers are people that attack/gain access into a system/networks illegally to see what is there and mostly to destroy data for their profits, to be malicious or just because it is there. Hackers usually gain access to a system through a network, but sometimes they physically enter a computer or network facility.

Business people should always keep their intellectual property from the eyes of their competitors or hackers, because much of the data is very difficult and expensive to generate. Therefore if care is not

taken loss or damages can put the individual out of business because networks are attack by morons. Consider what will happen when an enemy/hacker gains access to your network.

Network Security Measures Against Hackers

There are various ways and methods of protecting networks from dangers or hackers, and it is always very wise for not to rely on a single protection method and deploy them in layers designed so that an attacker has to defeat multiple defense mechanisms to perform a successful attack.

Below are some security measures that should be adhered to by all users of a network system:

Physical Access Control is the most basic level of security, but it is frequently forgotten. The most trivial way of stealing data or disrupting IT operations is to physically take or destroy pieces of equipment. Instead of spending more effort and resources securing your data against threats coming from the network, make sure to control physical access to critical servers and network infrastructure.

This involves the employing of security guards to monitor and guard the IT room/office so that nobody will have the direct access of stealing or damaging data or equipment and theft will not take place. Therefore the workplace should have tight security measure to prevent un-authorized people from invading the place. A padlock may be your most effective network security investment.

User authentication mechanisms are designed to uniquely identify users, assign their corresponding access rights to information, and track their activities. Workers should know that the security of the organization must not be compromised. User's ID and passwords are the primary means of safeguarding organizational assets.

Authentication is usually performed by challenging the user to provide access keys (passwords, biometric information, tokens, ID cards, etc) and checking their access privileges against a RADIUS, LDAP or SLDAP database.

Data Encryption is the process of encoding data through a series of mathematical functions to prevent unauthorized parties from viewing or modifying it. It has the objective to protect the confidentiality and integrity of the information, even when the encrypted data is in transit over unsecured media such as the Internet.

Data encryption works so that only the recipient can decode the data using the decoding algorithm that is not necessarily secret and an encryption key that is secret.

Network Packet Filtering is performed at network level and can be performed at routers and gateways by analyzing headers of IP packets and allowing or denying forwarding based on source or destination address, protocol type, TCP port number, packet length, etc. This is useful to prevent access even before there is an attempt to authenticate or look at system data.

Firewalls are devices that perform packet filtering but look beyond the Internet Protocol headers and also analyze the packet payload for patterns to deny/allow user.

The use of Passwords on data or the entire computer system can act as a protection from unauthorized people. A password has to be keyed in to gain access to the data or computer system and this is made up of characters, numbers, or in an alphanumeric form and the password is issued only to people authorized to use the system and this should be changed frequently to keep the data secure.

It is not advisable to use the name of the company or the owner's name or his/her family name as a password because many people might know this and others might try this to gain access to the data.

Restricted Access (privileges) to different data areas can be set up so that only authorized users can gain access to certain data. In this case all the users may be able to access the company's files, but access to certain data will be restricted to certain members, and this is done through the use of additional passwords or by setting up the system so that only certain terminals can gain access to certain data.

Back Ups: This is the act of duplicating files so that in case of any accident such as loss of original file, there will be copies/duplicates of the original, and if possible this duplicate will not be kept in the computer system alone or at workplaces but there should be more secured places to keep it.

Computer Viruses

A virus is defined as a small computer program that is capable of copying itself from one computer to another, thus emulating a biological virus that infects new hosts. Viruses are almost always written with malicious intent, and may inflict damage ranging from temporarily corrupting the screen display or slowing down the computer operation, through deleting certain files, up to erasing the entire hard disk content.

In certain cases intrusions occurs by way of software. According to Wikipedia, "A computer virus is a hidden program that alters, without the user's knowledge the way the computer operates or modifies the data and programs stored on the computer." It is said to be a virus because it reproduces itself, passing from one computer to another, or it can also enter a computer when a file to which it attaches itself is being transferred to a remote computer through a communication network and an infected disk or diskette will continue to spread the virus each time it is used. Other viruses take control of the operating system and stop it from functioning.

The most dangerous viruses do not act immediately after infection but often lie dormant for a long period until it is triggered by some event; such as reaching a particular date (Friday the 13th is popular) or running a certain program.

Writing a virus is technically demanding, so they are always written for the most popular brands of computer, where there exists a reasonable chance that they will replicate. Historically they have been mainly confined to IBM – compatibles Personal Computers and the Apple Macintosh.

The first virus was probably the 1987 Lehigh virus, followed by the more widely infectious Stoned, Jerusalem and Cascade viruses, all of which infected PCs running MS-DOS. These early viruses disseminated themselves via a floppy disk, copying themselves into the Boot Sector of the hard disk of any computer that was booted from that floppy. Their spread was exacerbated by the people taking floppy disks to work to play games, and exchanging pirated software on floppies. Once software became too big for floppies, this class of virus almost died out, as they can not infect the read-only

Compact Disk – Read Only Memory (CD-ROM). Now almost all viruses are disseminated via the Internet, either by the down-loading of files that they have infected, or hidden in an attachment to an Email.

There are three main categories of virus:

- (a) File viruses
- (b) Script or Macro viruses
- (c) Boot Sector viruses.

Protections against viruses

Scanning: This is a method by which virus-checking programs such as Norton Anti-virus searches disks and memory for known viruses.

Interception: This is a virus checking program that monitors processing, seeking to spot virus program in action.

Digital signature encryption: These are published programs that are encoded with mathematical key, making it difficult for virus to attack data or programs.

Health hazards & safety precautions associated with computer workplaces

Having a proper workplace and ensuring that workers enjoy the benefits a good and accident-free workplace is a good motivation for employees. It is very clear that a healthy and happy worker is more productive to any business. The key to designing a proper workplace for the knowledge worker is flexibility.

Computer operators/users are also covered by the health and safety act 1974. Therefore to comply with this act, employers are required to make sure that their places of work are safe environments. Issues related to the use of computers include the regular checking of all electrical equipment to make sure that it is safe to use.

It is also the duty of employees to undertake safe working practices and they are required to:

- Report any hazards relating to computers immediately and this could include trailing computer leads, loose wiring etc.
- Avoid lifting heavy equipments unless the individual is trained to do so.
- Take breaks at regular intervals.
- Maintain good posture when sitting at terminals.

Other related issues include:

The computer hardware

The Visual Display Unit (VDU): This should be located directly in front of the individual using it at his/her arms length with the top at forehead level and also outside windows should be to the side of the

VDU to reduce glare. The VDU should be high resolution with anti-glare screens and it should be free from smudges or dust build-up. It should also allow tilt/swivel adjustment.

Eyestrain

Constant use of the VDU can affect the user's eyes to avoid eyestrains for the users; the *following rules should be adhered to:*

- ✚ Staffs have the right to free eye tests before they start to work on a VDU screens and if possible they can also have a test after using the system.
- ✚ Screens should be free from flickering.
- ✚ Screens should not be placed where they reflect light.
- ✚ The user should be able to change the angle of the VDU.
- ✚ Lighting should be bright so that there is not too great a contrast between the screen and background light.
- ✚ Users should be able to adjust the screen brightness and contrast.

Keyboard

The keyboard should be located such that the upper arm and forearms are at right angle (90°), lie flat or an angle of about 10 degrees and it should be ergonomically design to accommodate better the movement of the fingers, hands and arms.

The keys should be concave shaped to avoid finger pains. The keyboard should not be attaché to the VDU so that the operator can adjust it to any height and angle.

Posture

Sitting at terminals for lengthy periods of time can lead to back, neck and arm injuries, and to help prevent such injuries:

- ✚ Chairs should be designed to swivel and move best if they have castors and should be adjustable for the individual user in the angle of the chair back and the height of the seat.
- ✚ Operators should have break frequently, because this for the change of posture.
- ✚ Chairs should possess armrests with height adjustment, lumbar support adjustment for lower back, and five –leg pedestal on casters.
- ✚ Arms should bend down from the shoulders and into angles at the elbow.
- ✚ Feet should be flat on the floor, with hips and knees bent at right angles.

The desk:

A wraparound workspace should be used to keep the PC, important office file and materials within about 18 inches of chair. Adjustable tray for keyboard and mouse and the tray should have height and swivel adjustments.

The room

Freedom of movement should be available for the operators; therefore there should be enough free space that will permit freedom of movement and ample legroom. The working room should be spacious for all the materials and the workers.

Warnings

Warning signs should be written and be provided in the workplace for customers and employees to see as a cautionary measure when walking around the place. An example is when the workplace has slippery floor, it should be clearly written mostly at the entrance so that anyone entering the place will be aware of the slippery floor and avoid rushing to prevent accidents.

No smoking signs should also be provided at the workplace, because it is not a good practice to smoke at workplaces. Therefore, it is the responsibility of the employer to make it known to both customers and employees that smoking is prohibited at the workplace.



Cabling & Wiring

During wiring, all wires should be protected using plastic insulators, and cables should not be scattered all over the workplace. This is to prevent accidents from electric current. Un-protected wires can cause electric chocks/electrocution and this should be properly taken care of in any workplace to avoid such dangers and accidents.

External security

For the external network security, this is highly required for a WAN (Wide Area Network) by setting up a firewall (e.g. De-militarized zone) is software that acts by

- a. Control access to your network from the outside
- b. Defines which part of the internal system can be seen from outside and also act in reverse - it can control any outside services visible from one machine.

Firewalls block incoming hacker attacks by using NAT (Network Address Translation) to hide much of the detail in network traffic so it looks like it comes from one machine.

The software can be set to prevent the screen traffic from:

- a. A pre-defined set of address
- b. A predefined set of users
- c. Traffic that contains certain type of data

These help protect the network from receiving unwanted or un-requested data packets, allow access to certain part of the system to users and lock other, even staff members can be provided with limited access and further more, firewall can be used as an anti-virus protection. Firewall also provides supports for encryption.

Internal security

Firewall plays a dual role as far as network security is concerned. It can serve as an internal as well as external security – it can control any part of the system that can be accessed from outside as well as within the organization. But must be operating systems support NTFS (Network File Server) which controls who has access to certain files within the organization. Logical securities such as passwords are needed to access files.

Health & Safety

Avoid costly accidents, minimize your liability and potential hazards, and meet published safety requirements by using comprehensive health and safety standards.

The promotion of Health & Safety at work must be a mutual objective for staff at all levels. We all have a duty to take proper precautions and care in our work not only to safeguard ourselves but also colleagues, visitors and contractors etc. within our offices.

It is considered essential in the interest of all employees, that they should observe and maintain the safety standards as laid down in this Policy.

Management and staff will be required to co-operate to maintain the health & safety at work of the workforce by observation of agreed practices and procedures for improved standards of protection for all persons using the company's premises.

Health & Safety must be regarded as a mutual objective for management and employees at all levels. Therefore management will:

- Provide and maintain safe and healthy working conditions in accordance with the Health & Safety at Work etc. all subsequent and relevant statutory requirements.
- Carry out suitable risk assessments of all premises and tasks carried out within them (to include the risks from fire, noise, manual handling, and exposure to chemicals & substances etc).
- Provide and maintain safe means of access and egress from all premises and locations.
- Provide safety training, information and instruction as required for all employees, visitors and customers etc, as appropriate.
- Provide all necessary safety devices, protective equipment and supervise their use.
- Maintain a constant and continuing interest in all aspects of safety, in particular by introducing and monitoring safety procedures, and involving employees or their representatives wherever possible.

Staffs have a duty to co-operate fully in the operation of this Policy by:

- Working safely and efficiently, complying with any instruction, information & training in accordance with all company procedures and statutory obligations.
- Immediately reporting incidents (including accidents, near misses that have resulted in, or may lead to injury).

Assisting with the investigation of accidents and aiding the introduction of measures to prevent a recurrence.

Conclusion

Having looked into various threats that lead to loss of access to corporate and individual data and some current solutions, I will like to conclude that computer experts need to sit down or go back to the Boardroom and analyze what is needed to protect, and how much can realistically be spent on that protection. The results should be a formal security policy that seeks to minimize the dangers from electronic threats, behavioral threats and acts of God.

It will inevitably be a compromise between the ideal and the minimum; but it must at least be achievable. It will define what users can and cannot do with their computers, and what outsiders should and should not be allowed to access. But it will also include behavioral rules for staff, to prevent accidents and social engineering. And it will also include general principles of good practice; such as back-up procedures and the use of uninterruptible power supplies. It is then we can turn to the hardware and software security solutions and ask the question: “what is the best system or systems to implement in order to meet these security objectives?”

References

IMIS Journal (1998). IT Security – Formulating a policy.

Terence Driscoll and Bob Dolden (1997). Computer Studies and Information Technology. Macmillan education Ltd: London and Oxford.

Wikipedia

WWW.Google.com