# Global Information Assurance Certification Paper

# END-USER COMPUTER SECURITY RESPONSIBILITIES... Know the rules of the game.

**Onwubiko Elekwachi**

**January 17, 2002**

## Abstract

This assignment focuses on the roles and responsibilities of the end-users in an organization, company or establishment were business activities are conducted using computers. I will begin this write-up by recounting an incident that occurred in an organization in the Southern Nigerian City of Warri. For security reasons, the name of the company in question will not be disclosed. End-users are employees and contractors of a company who use their employer's computing facilities. They are responsible for understanding and complying with the computing security standards and procedures of their company. These roles and responsibilities constitute part of an information security policy that I am developing. System administrators are advised to understand the driving principles and adapt policy to suit their organization. I have tried to minimize the use of computer/technical languages in the course of this write-up. End-users are advised to consult their IT technical support (TS) for explanations to computer terms. It is the responsibility of the TS group to ensure that adapted document is understood by every computer users.

## The Big Picture

Employees reported on duty one morning to discover that their external link utilization increased from the usual 45-60% to about 100%. This negatively impacted the quality of their services, especially the voice, since they had a 192-KB voice-over-IP link to a location in Europe. The support team spent some days establishing the cause of this service degradation. When it was understood that this search wasn't helping the situation, the security and controls team joined the help desk runners, visiting the clients and taking snapshots of applications installed on their systems. After about a day, it was discovered that the cause of the increase in link utilization was 'NAPSTER'. Some employees installed NAPSTER and used it to create MP3 CDs in commercial quantity. Test PCs were quickly setup and NAPSTER installed. With the aid of port analyzing tools, the security staff was able to get the TCP port this version of NAPSTER used for communication. Identified port was blocked and link utilization dropped to the usual level.

With the restoration of normal services, it was time for Management to sort issues out with the employees that misused computing services. The employees claimed ignorance of their roles and responsibilities.

It is worth convincing Management of every company of the importance of information security policy in their organization. Roles and responsibilities of both technical staff and computer users, constitute part of an Information policy. Definition of roles and responsibilities is required in every organization. In a growing nation like Nigeria that is just integrating into the Global Information Community, IT security awareness publications are required more than ever.

All computer users must understand that information security can no longer be a concern of technical specialists alone -- it must instead be addressed by a large team of individuals, including end-users and each of which makes their own unique contribution. Companies in the African region, where the advantages of information technology are just beginning to be

appreciated, cannot be left in this global move because a significant portion of computing takes place on the desktop. Companies rely on adherence to security and control standards to protect computing assets. Knowledge of roles and responsibilities will help you manage access to and use of your data and to properly control risks related to your business activities. In addition to data integrity, insufficient security could create a "safe heaven" for "the attacker in the middle". This is a situation in which an attacker compromises a less secure system and lunches attacks from it. Information security policies and procedures should help monitor compliance with standards and to assess the adequacy of the security standards and practices. Each user is responsible for protecting company-computing assets (property and information) that are assigned to or developed by him or her. All employees and contractors, regardless of whether they are computer users or not, are responsible for the assets and resources within their area of control.

All persons who possess sensitive information or who use a computer system to process sensitive information are responsible for safeguarding that information.
End-users must be aware of conditions affecting corporate assets, noting any problem or risk, and reporting them to their supervisor. They must also take reasonable actions needed to prevent damage or loss of company assets. Only individuals holding specific authorizations for access to sensitive information should access that information.

**Physical Security**

The physical security plan of any organization must ensure that access to offices, data centers and communication rooms is granted to authorized employees only. Other types of access must be under the supervision of an authorized person. Without good security plans, it is fairly easy for someone to get access to systems they are not supposed to have accessed by simply walking up to a valid user's desk. This can be the cleaning staff or a disgruntled (ex)employee making a visit. A cleaning staff once disconnected a device from the power source in order to power his vacuum cleaner. Guess which equipment was disconnected? The company email server whose UPS was sent for repairs the previous day.

Offices should be locked when personal computers and workstations will be left unattended for extended periods of time. If the PC or workstation has a built-in screen-saver password protection feature, enable the password when the PC or workstation is left unattended. If the PC or workstation does not have a screen-saver password protection feature, call your help desk for assistance. For Notebook/Laptop computers a BIOS or system password is required. The use of notebook cable lock is also recommended.

**Password Security**

The single most important end-user responsibility is to maintain the security of their passwords. Following are guidelines for selecting and using passwords. These rules should be enforced where possible on all company computing platforms.

- Choose passwords that are combinations of letters, symbols and numbers that have no meaning to anyone but you. The technical group must enforce minimum password length. Note that a password like **m2b:5y-A!** would take enormous computer resources and time to get cracked by any of the password cracking tools available on the Internet. This password

might seem very difficult to remember but if you interpret it to mean: **m**ade **2 b**abies **in 5 y**ears **with A**na! password becomes very easy to remember.

- Remember your password. Do not share your password. Do not write them down. Do not use software facilities for remembering or storing passwords.
- Change your password periodically. It is recommended that you should not repeat any password previously used.
- On some platforms, passwords are case sensitive and as a result, combination of both upper and lower case characters makes password more secure.

Following are practices that make passwords less easy to guess:
- Do not use acronyms associated with your company name
- Do not insert a number before or after a word or substitute a number for a letter (i.e., 0 for o, 1 for i or l, or 3 for e).
- Do not use names, even when spelled backward or with numbers appended.
- Do not use identification numbers (i.e., your Social Security number, street address, employee number or telephone number).

**Information Classifications**

Some information that originates in or is received by employees of a company contains sensitive business and/or personnel data that requires special protection.
Procedures must be adopted to safeguard such company information.
The following designations may be used for classifying company information.

1. **Class A**

Applies to materials containing operational, financial, or technical information, such as earnings statements, business investments, and assessments of the company's competitive position. Such information is intended only for a corporation and affiliate use.

2. **Class B**

Covers company information described above, requiring a very restricted distribution by the originator. Documents under this classification should be recorded in a Register which details title, date of dispatch, names of recipients, number of copies distributed, etc.

3. **Class C**

Designates information concerning company personnel records, such as background, salary information, medical records and performance appraisals.

4. **Class D**

The designation may be used to highlight material that does not contain competitive information, but should not be disseminated to the general public. Examples include company telephone directories, standards, and procedures.

5. **Class E**

This describes unclassified documents that are available to the general public.

**Transmitting Classified Information**
Ensure that the security classification of downloaded or file-transferred classified data is consistent with its source. An example of this would be sending or receiving a classified file as an attachment to a note.

**Choosing Storage Media**
From time to time classified information must be stored on electronic media. Data processed on the desktop must be protected according to assigned classifications.
Consider the security exposures of the various storage media and their associated controls before storing information in an electronic format. The following table summarizes recommended practices.

Recommended Data Storage Practices

| Media | Class A | Class B | Class C | Class D | Unclassified |
|---|---|---|---|---|---|
| **Floppy** | OK* | OK* | OK* | OK* | OK |
| **PC Hard Drive** | No | OK** | OK** | OK** | OK |
| **Network Drive** | No | OK*** | OK*** | OK*** | OK |

* Additional controls are required.
** OK if data is encrypted
*** OK if LAN restrictions are implemented.

Employees should also be aware that local hard drives may not be automatically backed up to the LAN and backup is the responsibility of the End-user. Additional controls (see below) may be recommended. Consider one or more of the following additional methods for protecting stored data:

- Physical locks controlling access to computing resources (e.g., cabinets, offices, and server rooms).
- Operating system-based access controls (e.g., NT file permissions.).
- Add-on software access control packages.
- Take appropriate steps to prevent disclosure of sensitive data before sending equipment out for repairs.
  Be aware of exposures to information on networked drives:
- Various LAN Administrative and Operator ID's can access any LAN files.
- Default settings in a company PC LAN standard load will automatically back up files on the PC hard drive to the LAN on a daily basis. LAN administrative personnel could access these files.
- ID's with "ROOT" privileges can access any UNIX workstation file.
- UNIX workstation hard drives may be automatically backed-up to the network and, therefore, subject to the same exposures as LAN files.
- Classify and label storage media based on the most sensitive information it contains.
- If possible, keep classified data on separate storage media from unclassified data.

- Ensure that sensitive data is removed from storage media when no longer needed or before equipment or media leaves your control. The DOS commands DEL and Format C: are not sufficient to delete data from storage media. The information must be completely eradicated by overwriting (called "Wiping" or "Wiped") or by destroying the storage media.
- Sensitive documents should not be printed on shared printers in common areas. If necessary, copy the files to a diskette and carry them to a secure system. Protect classified data while it's being printed.
- Consider data encryption for data with either high financial or business exposure.
- Clear unattended screens of sensitive data.

**Backup/Recovery**

Depending on risk, PC applications whose continued availability is important to the user may need to have backup copies of the application and data stored offsite. Recommended options are:

! **Storage on company LAN** - LAN files should be backed up daily and included in an offsite rotation schedule.

! **Storage on Mainframe** - Files can be uploaded to the mainframe. They are then backed up via normal mainframe backup procedures and subsequently stored offsite. Mainframe files can be downloaded very quickly. Costs may be higher than with other alternatives, but the convenience and simplicity of this procedure is significant.

**Computer Viruses**

Viruses are programs or code segments that are self-replicating. They can move from machine to machine through transfer of diskettes for program and data sharing. They can also be transmitted through electronic communications via networks including the Internet, bulletin boards, and e-mail systems. Some limit their activity to messages, graphics or mere existence, but the more malicious ones can destroy data or render a PC unusable. For this reason, virus detection program like McAfee, Norton, Dr Solomon etc. must be used on all PCs, including the memory resident program at startup. Memory resident program will scan files and diskettes for viruses without user intervention. I recommend its use by all personnel who move data or programs between home and office PCs.

For example, The McAfee software includes the programs SCAN and VSHIELD that can be executed at the End-users option before reading a diskette. SCAN is a user-executed program for explicitly searching a system hard-drive or diskette for viruses. VSHIELD is continuously loaded in memory and scans files as they are loaded into memory and diskettes before and while they are being read—it is automatic, but uses some computer resources.

1. **Exceptions:** Files currently open or being used by some process might not be searched by SCAN. This results in a non-critical error message.
2. **Updates:** From the statistic of the University of Houston-Downtown URL: www.dt.uh.edu/computing/uss/virus.htm, over 200 new viruses are being identified each month. Antiviral products require updating of virus data files to keep them current and as a result, computer users must perform the virus data file update for PCs on regular bases.

The proper use of virus detecting software by company computer users is very important to reduce the exposure to virus infections. Following is a list of "DOs" and "DON'Ts" to help.

- Do learn to recognize symptoms of a virus infection.
- Symptoms may include:
  ! Applications run more slowly,
  ! Unfamiliar messages or prompts appear on your display,
  ! PC response is erratic,
  ! Data is corrupted, and/or
  ! Inability of PC to boot.
- Do run the latest version anti virus software both at work and at home.
- Do scan all diskettes before use, particularly shared diskettes.
- Do keep a current backup of your data.
- Do hold down the Shift key when opening a file to prevent auto-start macros from executing.
- Don't use public domain or shareware programs on company-owned equipment without proper management approval. If approved, scan program diskettes before use.
- Don't reboot your PC with a diskette in the floppy drive.
- Don't leave a modem in "receive" mode unless you are expecting a transmission, and then, only if password protection or a security device is in place to limit access.

End-users are the first line of defense for protecting their machines from PC viruses. Any diskette used on home PCs or received from outside sources should be scanned before use on company PCs. If a virus is detected, you should:

- Stop work immediately but do NOT turn off or reboot your PC.
- Place a sticky note on the monitor of the PC indicating a virus has been detected and not to use the PC.
- Contact your Help Desk or information security contact person immediately.
- Make notes of everything you can remember related to the incident.

If you receive a virus notification and cannot determine whether a message is real or a hoax, please forward the note to your Help Desk. Hoax warnings are typically scare alerts to frighten recipients into mass distribution of the message, thereby jamming the networks with worthless messages. Forwarding messages about these hoaxes only serve to further propagate them.

Below is additional information about types of Viruses and some of their characteristics:

- Boot Sector Infectors (e.g., Michaelangelo, NYB) These move or overwrite the original **boot sector** of your PC, replace the boot sector with themselves, create "bad" sectors containing virus remainders, or infect your hard disk when you reboot.
- System Infectors (e.g., Lehigh). These viruses infect system files (IO.SYS, COMMAND.COM) and memory resident files.
- General .COM or .EXE Infectors (e.g., 1704, Scores, nVir) These viruses infect executable files (.COM or .EXE files) and may not become memory resident until the file is executed.
- Macro Infectors
  A type of virus has been identified that uses macro programming languages and infects applications and data files. The virus code is contained in auto-start macros that are attached to a file. A Microsoft Word for Windows 6.0 virus known as "Concept" is not destructive but saves documents as templates. Other macro viruses will surely appear. Any application that supports auto-start macros is susceptible (e.g., Excel, Word). Unlike older types of viruses,

these can be easily spread through exchange of documents, spreadsheets, templates, and the LAN.

**Acquiring Software**

Management approval is required for purchase of and installation of new software. Software licenses represent the right to use the software. Software use is restricted to the specific authorizations contained in the applicable software license agreement.
Software used outside the scope of the license agreement may result in a violation of copyright law and subject your company to substantial fines. It should be considered a serious offense attracting employee disciplinary actions.

**Notebook/Laptop Computers**

In the U.S. in 1999, 319,000 notebook computers and 27,000 desktop computers valued at close to $1 billion were stolen, according to Safeware, the Columbus, Ohio computer insurance agency (http://www.safeware.com). That same year, Fortune 1000 companies experienced losses of more than $45 billion from thefts of proprietary information, according to the American Society for Industrial Security. In the developing societies, thousands of people are ready to buy stolen and cheap notebook computers. Laptops have become part of the business world and as a result, they must be protected in other to protect important and proprietary information of a company. Bellow are suggested actions that would make your laptops more secure if they are followed.

- To protect software and information backup critical files and keep current copies readily available when traveling.
- Use BIOS password-locking programs.
- Use encryption programs or file compression with encryption programs if sensitive data are stored on the hard drive.
- Use anti-virus software. Scan all shared diskettes.
- Keep a record of your equipment's serial numbers. Always carry the notebook/laptop in a sturdy, weatherproof, and padded bag.
- Do not leave the notebook/laptop unattended overnight. Lock it in a file cabinet or take it with you.
- Place the notebook/laptop away from windows to prevent theft by breaking the window glass.
- Never leave the notebook/laptop unattended or out of your sight.
- Never check a notebook/laptop as baggage.
- Keep the notebook/laptop in your briefcase or carrying case while in the airport and entering/leaving the airplane.
- Keep a "proof of purchase" when traveling for Customs inspections.
- Take the notebook/laptop out of the briefcase only when putting the briefcase onto the x-ray scanner belt.
- Wait for any line at the metal detector to clear before allowing your briefcase or carrying case and notebook/laptop to pass through the x-ray scanner.
- Pass through the metal detector while the notebook/laptop is being scanned.
- Pick up your notebook/laptop and immediately return the notebook/laptop into its carrying case or your briefcase.

- If you set off the metal detector, wait for the notebook/laptop to come through the scanner, and ask the security agent to hold the notebook/laptop while you return through the metal detector or go on to the hand-held metal detector.
- Avoid storage in very cold or very hot weather.
- If a notebook/laptop must be left in a car, keep the car locked and the notebook/laptop out of sight.

**Personal Use of Company Computing Resources**

Company management intends that computer resources, such as PCs, workstations, and applications be used for business purposes. Personal use, therefore, should be incidental and must comply with company policies and procedures. Employees are advised to refrain from:

- Using company time to tour around the global village called 'Internet' Internet privilege is for the purpose of conducting company business.
- Monopolizing systems assigned to a number of users or located in the cyber cafe.
- Overloading networks with excessive data (spamming), wasting computer time, connect time, disk space. Downloaded music, games, video and executable files should not be stored in shared network drives.
- Wasting printer paper and toner, and other computing resources.

In some companies, license for Microsoft Office 97, Antiviral software and other applications allows home computer use by employees only and for business purposes only.

## Conclusion:

This part of your information policy provided a system for protecting information. Information is no longer simply something which supports the provision of a product or service. Information itself has become an asset. The establishment of roles and responsibilities are needed to properly manage and protect the information assets. To this end, this policy defined the information security roles and responsibilities of end-users.

I will conclude this work by citing 10 laws from Microsoft TechNet. Companies need a small army of well-informed employees for their computers to remain theirs for long. This publication should help equip this army.

The Ten Immutable Laws of Security

Law #1 - If a bad guy can persuade you to run his program on your computer, it's not your computer anymore.

Law #2 - If a bad guy can alter the operating system on your computer, it's not your computer anymore.

Law #3 - If a bad guy has unrestricted physical access to your computer, it's not your

computer anymore.

Law #4 - If you allow a bad guy to upload programs to your web site, it's not your web site any more.

Law #5 - Weak passwords trump strong security

Law #6 - A machine is only as secure as the administrator is trustworthy.

Law #7 - Encrypted data is only as secure as the decryption key.

Law #8 - An out of date virus scanner is only marginally better than no virus scanner at all

Law #9 - Absolute anonymity isn't practical, in real life or on the web.

Law #10 - Technology is not a panacea.

The bad guy here represents the attacker.



## References:

1. IT and Computing Services, UEA Norwich, "A guide to McAfee Virus Scan Software" "Jan 1999.
URL: www.uea.ac.uk/itcs/docs/d31.pdf

2. HHIC information Policy Committee, " Information stewardship policy," Nov 2000.
URL: www.hhic.org/hipaa/pdf/isteward.pdf

3. DRAFT chapter intended to be part of the NIST Computer Security Handbook. "Computer and Information Security Policy."
URL: secinf.net/info/policy/hk_polic.html

4. Microsoft Technet. Culp, Scott. "The Ten Immutable Laws of Security." Oct 2000.
URL: www.microsoft.com/technet/security/10imlaws.asp (Dec 29, 2000)

5. Network World, Inc, "Lessons in Laptop Security ". "March 2001
URL: www.nwfusion.com/net.worker/columnists/2001/0326zbar.html

6. Sophos Plc, Oxford, England " An introduction to computer viruses" , Oct 1999.

URL: www.sophos.com/virusinfo/whitepapers/videmys.html

7. Thomas R. Peltier. : Information Security Policies & Procedures .... A Practitioner's Reference, 1999, P10 -56

8. Donald L. Pipkin, Tulsa, Oklahoma, Halting the Hacker: A Practical Guide to Computer Security, Hewlett-Packard Professional Books, 1997, P200-214.

9. Andress, Mandy. Surviving Security: How to Integrate People, Process, and Technology. Sams Publishing. 2001. P30-51.