

Protecting Your PC: IT Security Awareness

By Louis Gamon

Whatever your level within your organization, or even if you work alone, you are responsible for the security of the data and information you work with.

Whatever your level within your organization, or even if you work alone, you are responsible for the security of the data and information you work with. This paper aims to provide those working on a personal computer (PC) with an outline detailing the proper custodianship of any and all information on the PC. As an introduction to the topic, this document may be especially useful as a tutorial aid; it may also be kept handy as a reference. It is applicable to your work or home environment, and applies to a PC owned by you or your organization.

The value of your PC is more than just the sum of the hardware and software; it's also about the type and importance of the information you have access to, through your PC and what you store on your PC – or carry around, if you use a laptop. Recent high-profile losses of very sensitive information potentially expose millions to identity theft. This demonstrates the importance of best practices, and some very basic control requirements.

It is therefore important that you know the reasonable steps to take to secure your PC and the information on it, in case of hardware malfunction, infection from malware, accidental erasure, natural disaster, unauthorized access or theft.

The objective and scope of this awareness document is to help you protect the PC and the information on it. We aim to:

- Look at the security risks you might face
- Provide you with advice that will help protect your PC (home or office)
- Provide you with advice that will help prevent unauthorized access
- Show how protective steps may be taken at an acceptable cost

Responsibilities and risk analysis

Just as we all have a responsibility for our own personal possessions – to lock up our homes and our cars – and not to disclose personal information such as credit card numbers and PIN numbers, except to those that have a need to know, we are all responsible for protecting corporate/company assets and information.

The questions you would ask yourself when looking to protect your own privately purchased PC would most likely be:

- Is this likely to happen to me? What are the crime statistics in this neighborhood? Are natural disasters common around here? Do I want family or visitors accessing my personal information (bank & tax details, private correspondence)? What sensitive information is stored?
- What's the actual value of this hardware, software and information to me?
- What's the potential impact of the loss to me?
- What's the consequence of someone else reading all the information? Would it damage me?
- How much will it cost me to replace the hardware, the software, the information? Am I insured?
- How much time would it take to recreate the information? Will it be easy, difficult or perhaps impossible?

In essence, you've just carried out a simple risk analysis of your PC environment to quantify the potential impact that you would suffer should your PC and/or information be stolen, damaged, destroyed or disclosed. Now: What preventative controls would it make sense to put in place—buy a new lock for the door, a strong cabinet to put the PC in when unattended, password-protect the PC and files, encrypt all files, and so on? We all have differing levels of peace of mind, so where do you draw the line?

Best practice (e.g., NIST, BS 7799) has laid down minimum criteria for the security of assets and information protection.

As you read through the following sections, ask yourself whether this is a risk you face. Do you handle or store sensitive information? Would observing some or all of the action items listed in the following sections limit or control the risks in your business environment? Are there other protective measures you ought to consider over and above these basic controls?

Intentional risks

Theft

The biggest threat to most corporations' PCs, especially laptops, is theft. Estimates for stolen computers are as high as 2000 a day, a 400 percent increase since 1997. You are most at risk from:

- Common and opportunist thieves looking to steal and sell the hardware or SIMMs/chips
- Someone who simply wants a better and faster model, and takes yours
- Unethical competitors seeking proprietary information, who target your laptop
- Hackers stealing PCs looking to find a way into your network – nodeNames, IDs, passwords

Virus attacks

They continue to evolve and become more sophisticated all the time.

Trojan horses

Beware of anyone bearing gifts or, for PCs, programs that hide nasty little visitors such as:

- Viruses
- Password grabbers
- Time bombs
- Keyloggers

Password grabbers

Once your password is known by someone else, your information is at risk. Internally this could be as simple as someone looking over your shoulder and then using your password and username to access the content of your PC. Externally this can range from individuals claiming to be system operators (this recently happened with Internet provider AOL) asking you to re-enter your password and observing what you type in; fake sign-on screens that capture your username and password; Websites that exploit weaknesses in Netscape and Internet Explorer to gain your password and username; and programs (executables) downloaded from bulletin boards whose sole purpose in life is to steal passwords.

Hackers

Once your password and username are known, an intruder can:

- Read, modify or delete information from your hard disk
- Load programs on your PC that capture information
- Use your PC as a jumping-off point to access other systems on the network

Unintentional risks

Acts of God

Each geography zone (Americas, Europe, Asia Pacific) has its own threats:

- Floods
- Fire

- Earthquakes
- Tornadoes

People

Yes, you and me. When did you last drop your laptop or spill coffee over the keyboard? Have you deleted files or folders by accident? Enough said.

Electricity

Most PCs tend not to like too much of it or too little of it. Switch yours off when leaving work.

Advice on measures to protect your PC

We've looked at the possible risks (threats). We also need to look at the information you access and/or store on your PC. The information you carry usually has a level of importance already assigned by the data owner which determines the classification of the data. Examples:

- Internal Use Only
- In Confidence (IC)
- In Strictest Confidence (ISC)

Or, you need to make this decision for yourself. That is, do you need to restrict this information from certain people? Would it be beneficial to your competitors? Would it reveal sensitive information about your employees and/or your customers? Would you be in breach of regulatory requirements?

So, what can you do to keep the risks to a minimum?

Marking and recording

Typically, each business unit is required to keep an inventory of all computer assets, by listing the type of hardware and the serial/asset number. All laptops and PCs should be clearly marked so that they can be identified as the property of "Company X." Clearly marking items will make them less attractive to a thief and also will aid identification. You can also use ultraviolet markers or chemical dyes, which will assist with identification and recovery. All of the above measures will assist in reporting theft, the follow-on investigation and the hoped-for recovery.

Physical security

The most obvious advice here will be to keep your PC in a secure place: a protected office environment, a locked room at home, protected by CCTV, behind card key access, or not on open display.

In addition, there are a wide range of devices available to help you protect your PC. For any laptop we recommend that you use a docking cable – a tie down. For those critical desktop PCs that you don't want to see walk, we recommend a lockdown unit, a secure box that bolts your PC to the desk or floor. There are also floppy-drive locks, keyboard covers, and audible alarms.

Action plan

The following actions are strongly recommended:

1. Store the list model and serial number away from your PC
2. Visibly and covertly mark your PC as "Group X" property

3. Fit and use a docking cable (non-breakable cable) on your laptop
4. Use a lockdown (secure cabinet) unit for high-profile or system administrators' PCs
5. Securely store your laptop when not in use – never leave it unattended and visible in the office, in your car or in a hotel room
6. Keep your backups physically separate from your PC
7. Request a security review of your work area if you have mission-critical hardware located there. Does it warrant more frequent walk rounds or CCTV in the area?
8. When traveling, store on the laptop only what you actually need for your meeting, and always encrypt sensitive data (Personal, Client, In Confidence)
9. When traveling, consider carrying your laptop in something other than an identifiable laptop bag
10. Report all losses, desktop or laptop, to Head of Group Security immediately

**Don't promote virus hoaxes and myths.
All alerts come from a recognized
security source – if you receive one from
a colleague, check it out with an official
source.**

Protecting your PC from virus attacks and Trojan horses

All PC users have a responsibility for ensuring that the systems they use are free from computer viruses and Trojan horses. On average, every month some 100 new viruses appear.

Anti-virus products

Use a reputable AV product – in the office, at home or mobile.

Action plan

The following actions are strongly recommended:

1. Install an AV product on all PCs you use for business data
2. Scan all files for possible viruses upon installing AV products for the first time
3. Always scan removable media before transferring files to your PC
4. Don't download executables from untrusted bulletin boards
5. Don't continue to send or distribute files once you know your PC is infected

**Request a security review of your
work area if you have mission-critical
hardware located there. Does it warrant
more frequent walk rounds or CCTV in
the area?**

6. Update your product with the new AV definitions (which check for new viruses) released by vendors daily – either via an automated process, or when informed
7. Use the BIOS setting to prevent booting from the floppy drive (A:)
8. Scan all downloaded files from the Internet or from online service providers
9. Don't promote virus hoaxes and myths. All alerts come from a recognized security source – if you receive one from a colleague or unknown source, check it out with an official source
10. Report virus incidents to your helpdesk

Advice on preventing unauthorized access

All PCs used for business purposes must have access controls that protect them from unauthorized access or use. This protection must address the following risks:

- Use of a PC without authorization
- Unauthorized access to files which are stored within or on a PC

Log-on banner

Your PC log-on banner must make it clear that the asset and information is the property of "Company X" and that unauthorized users are not welcome.

Controlling access to your PC

When you log in to your PC you are identifying yourself (with your username or ID) and authenticating yourself (with your password). If you then just walk away from your PC and leave it unattended, anyone can access and copy, modify, or delete your files, documents or folders; send email from you or your address; or put a password grabber or keylogger on your PC – to name but a few illegal activities. So don't leave your PC unattended – either always log out, or use a password-protected screen saver. Laptops have a "power-on" password feature, and we strongly recommend that you use it.

Passwords

User authentication today is typically by password. Anyone who knows how can run a "dictionary attack" against passwords, checking some 100,000 words in seconds. This can be performed internally and, with some considerable effort, externally. Use a strong password to prevent this type of attack from being effective. A strong password uses both upper and lower case, and uses letters, numbers and special characters. It has some length (minimum of eight characters), is changed regularly (every month or every quarter) and is kept secret.

Action plan

The following actions are recommended:

1. Use the “power-on” password feature if your laptop has one, and ensure it has been enabled
2. Enable the password-protected screen saver on your PC; alternatively, always log out when leaving your PC unattended
3. Create and use strong passwords
4. Change your passwords regularly, and don't reuse the same one
5. Do not disclose your password to anyone else
6. Always change your password if you think it has been compromised
7. In public areas, take care not to display customer information to prying eyes
8. If you have business-sensitive documents, find and use encryption
9. Consider using tokens, smartcards or biometrics (and Single Sign-On) rather than passwords
10. Use the BIOS setting to prevent booting from a floppy drive (A:)

Backing up your data

Users of PCs for business purposes must have appropriate recovery and contingency plans in place to fully recover all data. We've already looked at the things that can go wrong, and Murphy's Law states that if it can go wrong, it will go wrong. If all of your data is kept, accessed and backed up from your email server or office server; and you never – are you sure? – keep any information or data on your hard drive; and you or your service provider can easily recreate your PC environment or platform with little hassle; then you can skip this section. Otherwise, you are advised to read on.

We've established that you have information on your hard drive (C:) that you care enough about, should it be lost, to want to back it up. You are now effectively the system administrator, and need to acquire and learn the techniques to successfully back up your PC.

We've already looked at the things that can go wrong, and Murphy's Law states that if it can go wrong, it will go wrong.

Backups

What you back up, how you back it up (usually platform-specific), what you back up to (diskettes, CD, USB) and how often you back up depends on so many variables that you are the best judge. Remember, you are taking backups in order to recover the information or data should it be lost – whatever the cause.

Storage

Now that you've taken backups, ask yourself these questions. What information was on my hard drive? Was there anything that I don't

want disclosed? If you can restore this information or data, then likely so can other people, provided they can get their hands on your backups. So lock your backups away in a secure and trusted place, and not with your PC or in its vicinity – remember the fire or theft scenario! For very sensitive information, consider encrypting your backups.

Restoring

Don't fall into the trap of expecting everything to be perfect. Check that your backup did actually work. Restore a file or directory as proof that the information was backed up the way you wanted. Be sure you can restore the file or directory and read, modify or update.

Action plan

The following actions are strongly recommended:

1. Based on the volume of information to be backed up, choose the appropriate media. Ask your ISP for advice on supported backup devices that are suitable
2. For ease of backing up, place all the necessary files in a single directory
3. Familiarize yourself with your platform's backup features
4. Decide how often you want to back up, and stick to the plan
5. Label your backups “In Confidence” as the minimum classification
6. Don't store your backups with your PC or laptop
7. Do store your backups in a secure and trusted place
8. Remember that media are subject to heat, cold and magnetism, and treat accordingly
9. Remember that media does wear out. It doesn't have an infinite life
10. Test the recoverability of your backups – don't leave it until the day you need them

Conclusion

For a review of this awareness document in the future, look over the “Introduction” and “Responsibilities and Risk Analysis” sections to determine what questions you should be asking in order to fully protect your PC, as it operates in your home or work environment. This will provide the simple but necessary risk analysis. In each subsequent section, review the items listed to keep in mind those pertinent details of which you need to remain aware. Also ask of yourself once again, or of your organization, the questions posed under the section headings. Finally, scan over the “Action plan” in each category to evaluate which measures ought to be undertaken – and undertaken periodically, if necessary!

About the Author

Louis Gamon has 14 years of Information Security Management experience at the UK, EMEA and global levels working with Digital Equipment Corporation, AT&T and currently with YELL Ltd. (Yellow Pages). Louis formed the ISSA-UK Chapter in 2002-2003. As Regional Director for EMEA Louis supports some 15 chapters numbering 1000 members. In July 2005 he also took on the role of Chief Financial Officer sitting on the Board of ISSA International.