



Good Practice Note No. 4

IT User Security Awareness Seminars

Part of a series of notes to help Centers review their own internal management processes from the point of view of managing risks and promoting good governance and value for money, and to identify where improvement efforts could be focused. The good practices described in this series of notes should not be interpreted as minimum standards in every case, as not all may be appropriate to every Center.

INTRODUCTION

- Who causes physical and logical break-ins to computer facilities?
- Who writes computer viruses?
- Who steals passwords?
- Who causes vandalism, and malicious damage to computer networks?
- Who compromises computer networks and steal resources?
- Is it aliens from outer space?

No, the simple answer is men and women, and the biggest threat is from persons working in an organization. The greatest threats are not from the vagaries of the weather or earthquakes, but from persons, often those who occupy trusted positions within the organization itself, as fraud indicators have shown again and again. And one of the best security controls against this type of threat is a security - aware staff itself. Security awareness seminars are not just to make persons aware of the possible sanctions that might be imposed against them, but to raise their general level of awareness so as to add them to the fight against malcontents and unlawful intruders.



SUGGESTED CONTENT OF SECURITY OF AWARENESS SEMINARS

Physical Access

It must be explained why physical access to computer facilities is limited. The security policy must ensure that effective education has been given to holders of access permissions and that they are aware of their obligations, i.e. don't lend their electronic card keys, or allow friends to visit them inside the computer facility. All legitimate visitors should be escorted whilst on the premises and unknown persons should be challenged by staff. IT staff must be aware that a senior manager has no greater access permission than a clerk, if the manager does not have the required access permission.

Preventing Theft

Physically protecting a laptop presents many of the same problems that arise when protecting any valuable item. Since a laptop is a valuable commodity and yet needs to be openly accessed it is very easy for a thief to steal it or steal from data that might be stored on its hard disk, or even steal from its hardware components such as memory chips, hard disks, modems, etc. Users must be sensitized to these risks and examples given (from the Center's own experience, if possible).

Access Privileges

It should explain to users why they have access privileges to only parts of the system. 'Need to know' access privileges should be explained and the reasons that lay behind this strategy. The constant balance between granting enough access for the worker to do his or her job quickly and efficiently, and the need to impose restrictive controls should be drawn out and examples given. The reasons behind password 'hardening' and access lockout strategies should be explained. It must be emphasized that access to the Internet is a privilege and not a right and that users must abide by regulations governing access to pornographic, music, gambling and hacker sites. Sanctions that can be imposed must be explained in detail and any relevant promulgated policy referred to. Details regarding preventive and detective controls over access to unauthorized sites could be touched on in a general way, without sufficient information been given to allow the user to circumvent the controls in place. Users should be made aware of the Center's email policy and the reasoning behind it.

Viruses

Viruses and virus control can be explained in a general way and the various types of virus discussed. Participants should be encouraged to discuss their own experiences with viruses (the writer of this paper lost a hard disk full of data to the Michelangelo virus, which struck on the date of the artist's birthday).



Use of personal, pirated, and downloaded software

The Center's policy in relation to the use of personal, pirated, and downloaded software should be explained, as well as the reasons underpinning any restrictions imposed on users in regard to this class of software. Users should be made aware of the risks in sharing private non-work related passwords and access codes, and should be told that they need to report any loss, theft, or abuse of these, as this may affect network security.

Hackers

Users should be made aware of the different methods used by hackers, and some of the motivations behind this type of attack. It is not always bloody-mindedness but at times, out-right theft of computer resources and/or bandwidth. Controls used against hacker attacks could be discussed in a general way, without divulging specific methods used by the Center.

Exposure Draft: March 2003 (Adopted without change)
Author: Gerry Reardon