



ASCIP *RISK ALERT!*

Date: October 10, 2006

Attention: ASCIP Members

Subject: Protection of Sensitive Documents

ASCIP continues to receive claims related to the theft of desktop computers during burglaries, the loss of laptop computers through theft or inattention, and requests for assistance regarding the loss or misappropriation of confidential information which was stored on lost or stolen equipment or has otherwise found its way outside of the areas where it was intended to be.

The loss of physical computers, network server, and/or related peripheral devices typically falls under ASCIP's Electronic Data Processing (EDP) coverage, subject to the applicable deductible, however the work products and data on those machines are considered intangibles and generally not included in such coverage. Similarly misappropriated, lost or damaged information or data from a computer or network would generally not be covered nor would the consequences of its misuse.

The need to protect sensitive personal information from loss or unauthorized access is well known and has been the subject of much attention in the media. Every level of government and private industry has suffered the consequences of unauthorized access to or loss of such information and the potential for identity theft. Both State and Federal laws require timely disclosure of unauthorized access to personal information held in electronic databases.

During 2006 ASCIP members have reported burglaries in which desktop computers have been stolen from human resources, payroll, benefits, insurance and other areas which may contain sensitive personal information. On visits to various district offices, ASCIP's security consultants have reported sensitive information left unattended on desktops, in office waste baskets, and on unattended computer screens. Many laptop computers have been stolen from vehicles in which they were left in plain view. Desktop computers in administrative areas are generally not locked down to prevent theft although in many computer labs and classrooms such machines are usually secured.

Other findings include the use of common passwords by employees and temps to access computer files, some of which should be restricted to those with a need to know. Where passwords are used, they may not be changed on a regular basis or may be posted at the workstation for easy user recall. Some district internet access points lack fundamental protection from attack by computer hackers who have accessed both staff and student records, obtained home addresses, changed grades, introduced viruses, and damaged files during their intrusion efforts.

ASCIP encourages its members to discuss these and similar concerns with their information technology staff and investigate preventative measures such as encryption of files containing personal data, physically securing administrative computers to prevent theft, instituting effective password or biometric access programs, conducting cyber security audits, shredding sensitive materials, and other proactive measures. ASCIP may be able to assist in these activities. Please feel free to discuss your needs with an ASCIP staff member!