不容忽视的五个角落

角落一：某单位收到一份加密传真，内容是《节日放假安排表》（非密），呈送领导后，业务参谋将其随手扔到了废纸篓里。

误区：《节日放假安排表》没有密级，不属于军事秘密，可以随意处理。

正解：《节日放假安排表》内容本身虽不带密，但其是由密码装备加密传送，乱扔会影响密码安全。处理这类非密文件，要么妥善销毁，要么按涉密文件资料管理。

角落二：某部网管为维护本级涉密网站，经常利用保密管理系统服务端可读取加密和不加密U盘的功能将内网和外网数据进行导入导出。

误区：通过保密管理系统服务端传递数据不会造成失泄密。

正解：若内网计算机感染了“轮渡”木马，该病毒同样可以利用保密管理系统服务端可读取加密和不加密U盘功能形成的隐秘通道，将涉密信息“带走”。非涉密网和涉密网数据交换可以通过刻录光盘完成，应按其存储内容中密级最高的管理方法进行管理。

角落三：某单位对接入涉密网络的计算机进行保密检查时，只检查系统有无安装“保密系统”，是否设置双重密码，有无防病毒软件等，而不检查系统中是否存在安全漏洞以及是否打补丁。

误区：涉密网络属于内部网，与互联网物理隔离，而修补系统漏洞的主要目的是防止攻击，打补丁只会让系统越来越慢，加之系统中已经安装了防病毒软件，所以不打补丁不会对系统安全造成影响。

正解：涉密网络虽然与互联网物理隔离，但其中同样存在大量的病毒以及各种攻击，如果对方通过漏洞攻击取得系统的控制权，很可能从内部瓦解系统的防御体系，并且在用户不知情的情况下窃取计算机中的资料。所以，系统漏洞的修复不容忽视。

角落四：某单位将传真室报废的打印机直接卖给废品收购商。

误区：打印机已经损坏和报废，不涉及任何秘密，且不属于涉密载体，当废品处理不会造成失泄密。

正解：打印机都会有小容量的存储部件，类似计算机硬盘，在打印涉密文件资料时，这些文件资料将会存储在该部件上，所以报废打印机时应当分离或物理销毁其存储部件，或者用普通文档将存储部件中的内容反复覆盖，而后作报废处理。

角落五：某部保密员将感染木马病毒的计算机重装系统（只将系统分区进行格式化）后，继续使用。

误区：重装系统后，病毒就不复存在了。

正解：目前，大多数木马病毒都可以将自身复制到硬盘的所有分区并且隐藏，有的甚至会感染和捆绑常用的数据文件，更有甚者会潜伏在硬盘引导区，如“鬼影”病毒。重装系统不代表消灭病毒。重装系统前最好先转移数据，重新将硬盘分区，并通过PE或其他方式查杀引导区病毒，然后再重装，并做好计算机的相关安全防护。

来自：《上海市保密局门户网站》