**不要随便“修电脑”，泄密隐患藏其中**

随着信息设备技术的广泛应用，因违规进行信息设备维修导致的失泄密事件时有发生。

**典型案例 揭示三大风险**

**送外维修易失控**

2013年6月，有关部门发现，某计算机服务公司计算机中存有某局相关的多份标密文件和上千份内部资料，给国家秘密安全造成严重威胁。经查，系该局办公室主任闫某于2009年5月违规将故障硬盘送至某电脑公司维修，后又转至该计算机服务公司，造成涉密文件失控。

**雇人维修有风险**

2016年11月，某机关单位2台涉密计算机发生故障，无法连接内部局域网。因当日网络维护技术人员生病住院，经单位负责人尼某同意，工作人员姬某联系某办公设备公司售后服务人员进行维修，维修人员在不知情的情况下，将涉密计算机连接互联网，导致多份内部文件外泄。随着信息设备技术的广泛应用，因违规进行信息设备维修导致的失泄密事件时有发生。

**不闻不问酿大祸**

2009年4月，某单位一台涉密复印机发生故障，请售后服务商派人维修。修理人员经过简单测试后断定是复印机硬盘问题，须将其带回维修。该单位有关工作人员毫无保密意识，让其带走维修，且没有落实旁站监督要求。几天后，该单位才意识到存在保密隐患，立即与售后服务商联系，方得知该硬盘已被送往境外，导致涉密信息失控。

**防范对策 捂住失泄密跑风口**

其实，纵观上述案例，案情或有不同，但诱发问题的原因却是一样的：

其一，相关人员对维修工作的认识存在偏差。设备出现故障，工作人员往往通过网络、朋友四处寻找维修人员，不能冷静联系定点维修。很多工作人员只关注设备功能是否恢复良好，而对让谁维修、如何维修等问题并不关注。

其二，相关单位对维修工作管理不够严格。比如，对涉密信息设备数量记录不清楚，标识不明显，在使用、维修等方面不够规范；执行保密制度随意性大，落实不到位；没有指定维修单位，工作人员遇到设备故障过分迷信品牌售后服务，没有及时联系单位信息化或保密部门解决，等等。

（原载于“保密观”微信公众号）