安全性

□ 对信息系统安全性的威胁

任一系统，不管它是手工的还是采用计算机的，都有其弱点。所以不但在信息系统这一级而且在计算中心这一级(如果适用，也包括远程设备)都要审定并提出安全性的问题。靠识别系统的弱点来减少侵犯安全性的危险，以及采取必要的预防措施来提供满意的安全水平，这是用户和信息服务管理部门可做得到的。

管理部门应该特别努力地去发现那些由计算机罪犯对计算中心和信息系统的安全所造成的威胁。白领阶层的犯罪行为是客观存在的，而且存在于某些最不可能被发觉的地方。这是老练的罪犯所从事的需要专门技术的犯罪行为，而且这种犯罪行为之多比我们想象的还要普遍。

多数公司所存在的犯罪行为是从来不会被发觉的。关于利用计算机进行犯罪的任何统计资料仅仅反映了那些公开报道的犯罪行为。系统开发审查、工作审查和应用审查都能用来使这种威胁减到最小。

□ 计算中心的安全性

计算中心在下列方面存在弱点：

1.硬件。如果硬件失效，则系统也就失效。硬件出现一定的故障是无法避免的，但是预防性维护和提供物质上的安全预防措施，来防止未经批准人员使用机器可使这种硬件失效的威胁减到最小。

2.软件。软件能够被修改，因而可能损害公司的利益。严密地控制软件和软件资料将减少任何越权修改软件的可能性。但是，信息服务管理人员必须认识到由内部工作人员进行修改软件的可能性。银行的程序员可能通过修改程序，从自己的帐户中取款时漏记帐或者把别的帐户中的少量存款存到自己的帐户上，这已经是众所周知的了。其它行业里的另外一些大胆的程序员同样会挖空心思去作案。

3.文件和数据库。公司数据库是信息资源管理的原始材料。在某些情况下，这些文件和数据库可以说是公司的命根子。例如，有多少公司能经受得起丢失他们的收帐文件呢?大多数机构都具有后备措施，这些后备措施可以保证，如果正在工作的公司数据库被破坏，则能重新激活该数据库，使其继续工作。某些文件具有一定的价值并能出售。例如，政治运动的损助者名单被认为是有价值的，所以它可能被偷走，而且以后还能被出售。

4.数据通信。只要存在数据通信网络，就会对信息系统的安全性造成威胁。有知识的罪犯可能从远处接通系统，并为个人的利益使用该系统。偷用一个精心设计的系统不是件容易的事，但存在这种可能性。目前已发现许多罪犯利用数据通信设备的系统去作案。

5.人员。用户和信息服务管理人员同样要更加注意那些租用灵敏的信息系统工作的人。某个非常无能的人也能像一个本来不诚实的人一样破坏系统。

□ 信息系统的安全性

信息系统的安全性可分为物质安全和逻辑安全。物质安全指的是硬件、设施、磁带、以及其它能够被利用、被盗窃或者可能被破坏的东西的安全。逻辑安全是嵌入在软件内部的。一旦有人使用系统，该软件只允许对系统进行特许存取和特许处理。

物质安全是通过门上加锁、采用防火保险箱、出入标记、警报系统以及其它的普通安全设备就能达到的。而作为联机系统的逻辑安全主要靠“口令”和核准代码来实现的。终端用户可以使用全局口令，该口令允许利用几个信息系统及其相应的数据库；终端用户也可使用只利用一个子系统或部分数据库的口令。

□ 安全分析过程

大多数公司的办公人员询问关于信息和计算中心的安全时，往往问“一切都行了吗?”其实他们应该问“对于信息和计算中心的安全，我们应该做什么?”。

用户管理人员应该与信息服务管理人员定期地共同研究，进行安全分析，这种安全分析为各方都愿意接受。简言之，这种安全分析意指决定要多大的一把“挂锁”。遗憾的是，某些公司乐意承担巨大的风险，但又侥幸地希望不要出现自然灾害或预先考虑到的祸患。“难得出现”并不等于“永不出现”，关于这一点某些公司发现得太晚了。

在进行安全分析的过程中，用户和信息服务人员要切实地审估几十种安全项目清单是否

充分。例如，在属于物质安全方面，分析组可能要调查通向机房的路径数目，或者要调查是否存在一张进入机房的特许名单。

安全分析方法的步骤如下：

1.估价危险。(1)识别和分析薄弱环节。(2)确定特定事件出现的概率。

2.危险审定。在估价危险的基础上确立可接受危险的标准(信息系统的安全是按一定的程度来实现的)。

3.减少危险。(1)把对薄弱环节的威胁减到最小或消除它。(2)重复第 1、第 2 和第 3 步，直到这种危险小到可接受的程度。