微型計算機的數據安全問題及其對策

曹德明 江敏 張正興 譯　瞿兆榮 王建慶 校

Microcomputer Data Security

Issues and Strategies for Business Daniel J. Cronin

華東計算技術研究所

译 者 序

随着计算机应用的深入发展、计算机的安全问题已显得日益突出。尤其在微型机应用普及的情况下，一方面由于微型机缺乏大型机系统所具备的较强的内在安全功能，另一方面还由于微型机用户缺乏计算机安全保密知识，因此，有关微型机数据安全保密问题更是广大微机用户所面临的迫待解决的难题。

《微型计算机的数据安全问题及其对策》一书是美国作者Daniel J. Cronin 1986年撰写的。全书共有十三章，阐述了有关计算机安全知识和计算机犯罪情况；介绍了硬件防盗、电源保护、自然灾害及环境防护等安全措施；论述了数据后备的重要性及其必要的知识。本书在指出DOS操作系统的不安全性同时，详细地介绍了适用于IBM PC数据安全的实用程序、存取保护和数据加密方法；列举了用于微机存取控制及数据加密的硬件设备和专用软件包。此外，本书还涉及有关微机通信连网的安全保密问题，各种管理控制方法及管理安全问题。

全书内容丰富，能结合IBM PC机使用实际来论述微机的数据安全问题及其对策，将有助于广大微机用户掌握安全保密知识，提高用机的安全水平。

为了将本书尽快出版以飨读者，前言、第一、二、三、四章由江敏同志翻译，第五、六、七、八、九章由曹德明同志翻译，第十、十一、十二、十三章由张正兴同志翻译，並由瞿兆荣、王建庆两同志对全书进行校对。由于译者水平有限，翻译定有不妥之处，望读者批评指正。

译 者

一九八八年九月

前　言

神话与现实，安全与不安全，正确与错误——围绕着微型机安全方面的截然相反的问题。全球性的微型机社会已遭到这些矛盾的袭扰，因而对微型机社会的安全究竟会受到何种程度的破坏，产生了许许多多的误解。

去年夏天晚些时候，我在漠然观看晚间新闻时，一则报道引起了我的关注。报道说，佛罗里达当局又搜查到一个由少年行窃者（hacker）集团设在郊外的总部。据称他们这些人已钻进政府设施内部去了。一开始，我为此感到惊愕——这不会又是一起行窃者的围攻事件吧！但是，听着，听着，我很快感到恼怒而又难以相信了。据报道，当局认为这些着了魔的行窃者对利用电子技术使北大西洋组织的卫星在外层空间里偏离轨道数千英里应负有责任。

本书便是我对许多有关计算机安全神话的挑战。我始终如一的目的就是要消除这些神话，并代之以事实。

编　者

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

第一章 概 述

现实——微型机不受检验而大量涌现出来，而其之脆弱易受攻击渐渐使我们处于纠缠不清的境地。

现实——1986年运往主要大城市地区的PC机总数可望达到650万台。

现实——1985年末，在全美国内有近150万台PC机连接在局域网上。

现实——全国各地300多万台微型机在各自的家里发出阵阵欢乐的嘟嘟声，而同时又都在焦急地等待。

现实——1983年发运的安全产品总共为26亿美元，预计到1988年发运额将猛增到44亿美元以上。

现实——计算机犯罪是全国发展最快的行业。以报导的各个案例罪行，取其平均价值就超过10万美元。

在过去的整整两年中，涉及微型机的耸人听闻的犯罪案例已被广为宣传。最为轰动的案例之一就是涉及密而沃基市的414行窃者（HACKERS）俱乐部一案。一批着了迷的杰出青少年自夸闯入了60多台商用和政府部门的计算机。

1984年后期，在相当一段时间内，TRW信用局被闯入丑闻达最高纪录。宣传报道机构更加努力追随（着重于幻想式的）好莱坞幻想片“战争游戏”，如该片是描述一位具有桃色新闻的青年，他出于巧妙干预和盲目大胆碰运气竟使全球浩劫。每件实例的报道内容纯属于过度夸张和歪曲，前后的报道自相矛盾，逻辑不合。然而某些有价值的思想随着这种超越而产生——对计算机安全的日益醒悟；或者是意识到计算机到底是否安全的问题。

一、什么是计算机安全

大小公司的经理们在某些令人痛苦的现实面前正觉悟起来。各公司对IBM PC机的依靠性与日俱增，广泛用于追踪存货情况，监测销售报告，规划发展战略，进行产品设计、储存专利秘密，开工资清单，管理支出和收入等。而现在突如其来的是，不知何处冒出了这样一个奇怪的问题：“我的系统到底有多大安全？”

事实上，任何两个安全方面的专家对计算机安全的精确定义都不会取得一致意见的。这不因为计算机安全是门难以理解的学科，而是它涉及到如此之多的因素：物理安全、计算机维护、硬件的防盗保护、数据完整性的控制、高度机密数据的分类、数据存取控制以及用户的授权等等。一般人的认识是常把计算机安全与计算机犯罪混淆起来。因为没什么东西比事实更有说服力。

下述的计算机安全定义可算是完整概括，也是本书出发点和指导准则：

安全性是指你所拥有的计算机一直是由训练有素的合格人员和专人安全操纵的，而计算机系统本身以及所有的程序和数据必须是受到保护的。

最后，安全性意味着任何输入的数据能在将来随时随地检索，并不因为故障或故意的行为而有所改动。

二、安全作为管理的一个课题

微机安全尚是管理上的空白点。尽管意识到安全方面的威胁感与日俱增，但是经理们基本上仍未对这个问题引起足够的重视。公司的各级管理部门，无论是管理人员还是执行经理都必须了解这一知识。

部分问题如计算机本身的故障，雇员的欺骗，或是计算机软件中的潜在错误造成处理出错，常常是隐含的不明显的，且需很久才会暴露出来。由于无"冒烟枪"可告诫他们。要充分认识管理上的潜在危险是困难的。在许多场合，安全受到破坏都是偶然被发现的——窃贼们自己放出风来。下面Zwana的下舍入欺骗帐户是最好的例证：

1.Zwana帐户

好几宗像这样典型色拉米香肠式的诈骗案（下舍入数额的窃取）已多次报道过了。人们都在猜测到底已有多少这类犯罪案例，但是渐渐地人们又忽视这一令人为难的问题。这种色拉米香肠技术虽已老了，但全体查帐人能重新描绘出某些笨拙的方式。

十三世纪的威尼斯商人就开始用两本分类帐册来保护自己免遭这类欺骗。

Zwana一案经过是这样的：加利福尼亚南部银行的一个程序员某一天得出一个有益的新发现。他意识到银行系统计算用户的利率是算到千位，但又舍到百位数，计算机对舍去数字的利率忽略不计。这位程序员不愿看着这批钱被浪费，因此他写了一个插入码（计算机的程序加入了秘密指令），这样银行里每个客户的额外利息都滚进了一个以Zwana命名的伪造帐户里。三年中，他高兴地收集起便士、换成百元，然后上千元，直到阴谋诡计意外地被查出。银行的市场部表演了这系统出现的奇迹。然后把最后面的名字Zwana写进了文件。但对他们来说，更为难的是Zwana根本是不存在的。

不幸的是，管理中的迷信做法成了一个特点。安全常置于不太受重视的地位，因为经理们宁可深信是那个过马路的家伙将被撞倒，而决不会是他们自己。由于不会被撞倒，那又何必把钱浪费呢？

所有归集到一点就是：是否在自己的车被撞毁后才去保险车呢？在安全上采用这种沉溺于侥幸的策略则是短命的。

不久前，我会见了一位对安全具有独到见解的高级经理。他雇了一名安全顾问，并确信这顾问将给他们的公司带来丰富的经验，因为他认为已经到了易犯某些原始错误的时候了，但他决不再重复他人已犯的错误。

在今天这样信息爆炸的社会里，关键是人们离不开计算机。成千上万台计算机遍及整个大陆，使人们与办公室、局、机关科室、甚至家庭连接起来。在全美国，每年个人机的增长呈指数地上升。随这种增长伴随而来的是令人惊愕的控制问题，一个分散化带来的恶梦。是谁正在运行？运行什么，在什么机器上，在什么时候，什么地点等等，且又是为什么？

三、风险管理时的安全问题

有成效的经理一定是个魔术大师——他深知平衡的真正含意。安全问题是风险经理的职责。任何需要决策安全问题的经理，我们可称他为风险经理。风险经理好似一个手拿纸牌的赌徒，但他的工作是要确切知道什么在危险之中。风险经理对安全级的选择必须基于本公司对计算机系统的依赖程度，换言之，要估计到如果遭受最大的破坏，公司将会垮到何种程度。

风险经理必须估价本公司对自己系统的依赖程度，多考虑实质性，少顾及表面性。必须制定出系统的全面恢复策略，并且对任何事不要期望过高。

什么才是易受破坏的微型机的真正风险所在呢？以下举几个例子：

·有不满情绪的雇员对计算机硬件、软件或重要数据的破坏。

·由于停电造成对计算机硬件、程序或数据的损坏。

·丢失未获专利权的职业秘密和开发中的产品设计方案，落入竞争者手中。

·泄露私人及有潜在区别对待人员的记录（如有酗酒史或医治精神病的记录）。

·泄漏人员的薪水。

·改动或删去公司多月甚至多年存贮在磁介质上的重要数据——财政记录、利润收入、销售合同。

·出于贪污或欺骗的目的，故意使数据输入出错。

风险经理的工作不易，也并不令人羡慕。尽管公司的信息资源全由他负责，但风险经理也不能变为谨小慎微的胆小鬼。对于最初的破坏和威胁，风险经理往往表现出危机的情绪和过于妄想。风险经理在策略的形成之际，公司的数据库仿佛位于被火山埋掉的意大利古都——庞贝的城基上，是不会立即卓有成效的。

如果计算机系统通常是用作字处理，那么风险经理不必调查昂贵的存取控制系统或是摄像监视器及保护装置，也不必去毁掉未用的打印输出结果，否则将难以辨明。但是，如果同一系统保存着公司帐目清单，保险自然要升级。有高度机密信息处于危险之中，风险经理此时必须要提高要价，以求对安全措施的代价与竞争所需的高度机密数据的丢失风险加以平衡。

最重要的是对平衡的设想。这样，风险经理才能着手对安全保险进行估价，并设计一个适合于自己特定环境的合理安全程序。下面的准则若能谨慎应用能起很大的作用：

决不在安全数据方面花更多的钱，而宁可承受丢失这些数据的代价。

看来在这个世界里不会有人愿花钱来保护自己的个人计算机。但也有代价相对不太贵的解决办法。当然，至今尚未发现在公共域（Public domain）中有哪一种可用的珍贵软件竟几乎是不花费钱的。所有在本书内各处引用的公共域软件程序是由加利福尼亚州Sunnyvale的IBM PC软件小组的安排下得到的。目前混乱分散于成千上万个程序中与安全相关的程序被独立存放在一对软磁盘上是有益的。所有引用的公共域程序都附入本书末的附录A中。

四、安全作为防御手段

IBM个人计算机的安全问题实际上是一个防御问题。单个保护措施是远远不够的；相反，足够的防御则要多层次的保护。

在中世纪的欧洲，城堡的设计是为了抵挡敌人的侵犯。退却防御系统是建造成环状形或是“城楼”、壁垒和护城河。由于防御者是从城堡的外墙退至城楼——城堡中心，庭院和王室住处——他们的防御强化了。敌人只好加倍努力并采取不同的进攻计划来排除这种接二连三的障碍。

城堡所处的位置要有360度的视野观看到村庄、田野。敌人在阳光下无法藏身，必定是无法靠近。晚上攻击者不可能游过护城河，否则会发出声响被他人发现。

壁垒里的防御者具有居高临下的极好的作战位置。这种物理上的障碍物是难以攻克的。要么破坏城墙或是爬梯才能越入，不过，射手们可迅速消灭企图越墙的入侵者。

如果进攻者能坚持到打败抵抗者为止，那就能进入城墙，然后攻击城楼了。这时生命的价值相当程度取决于规模，与征服的战利品相比，力量基本相当。只有艰巨的攻城训练和火炮才能蔑视城楼的安全防御，因为要攻击城楼和内部密室需付出重大代价。

IBM个人计算机的情形类似于中世纪的城堡，也应该得到集中式的环形防御。这些防御环的各自工作状态又要与其他环相联系。防御中的某一区域力量不强就会削弱整个系统的安全程度。

在这本书中，我们将一一叙述这些安全防御，如：清查干预，排除险情。在此首先描述安全防御所涉及的范围。

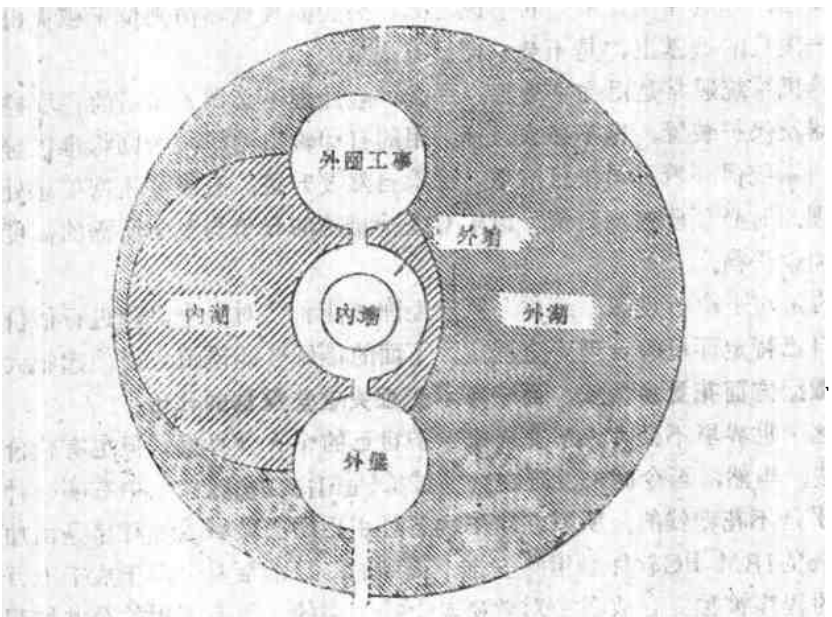

图 1.1　中世纪城堡防御

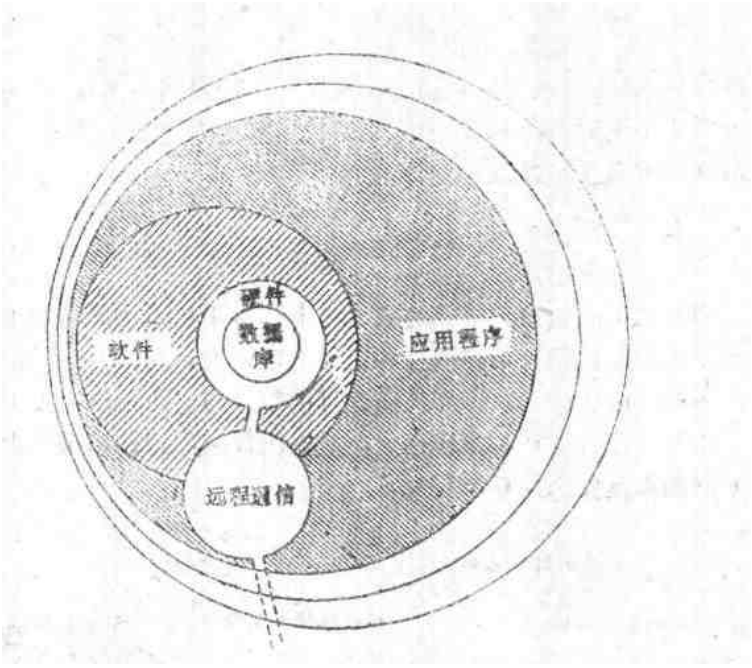

图1.2 微型机系统防御

1.物理环境

物理环境是指最外环的防御，即保护个人计算机，所有的外设、存贮介质（磁带、软盘）、工作站以及与工作站有关的物理存取。对个人计算机的环境设计将会限制认可的存取用户，并且通过对仪器和报警信号的控制，可以阻止罪犯。为此，计算机应有的保护是不受环境威胁，如：泄漏、火灾、破损、盗窃和捣乱。

2.应用程序

应用程序是管理大量的数据处理和一些工具，例如：微机数据库系统，电子试算表、字处理和工资管理程序。带有安全意识的应用程序就会编入控制码，防止欺骗性的处理，输入／输出错误，以及未经许可的存取数据文件。现已具备为安全起见而严格设计的程序，涉及范围从简单的口令保护机制直至复杂和升级的口令保护机制。

3.远程通信

远程通信对计算机系统的安全保障是令人麻烦的附加物，调制解调器逐渐巧妙地挤入介于应用层和PC机操作系统间这一级，如果不加以保护，那么它就会通过薄弱的环节向未授权的用户告密，并攻入系统核心，无耻地进入数据库。远程通信保护的核心是要用户确认：即我们如何知道用户自己所说的身份？为了确保远程通信的安全，对硬件和软件加以控制是非做不可的苦事。

4.操作系统

这一层的系统软件是在硬件之上活动的，一般允许访问硬件和已存入的数据。所有的计算机资源——存贮、处理、数据传输——是通过操作系统提供给应用程序和用户的。如PC—DOS是一个复杂的动物。不过，一旦熟悉DOS，也能操纵它来加强个人计算机的安全。另一方面，DOS也能胜任对付不良的企图。

此为试读，需要完整PDF请访问：www.ertongbook.com

5.硬件

硬件构成最内环，它是系统食粮——数据——的最后一道保护。硬件配置具有内置式的可靠性方面或是电源故障的保护。人们可以用各种各样的方法修正硬件配置，从而提高系统的可靠性，并且保护私人数据库的完整。

五、技术——全能的万应药吗？

正是我们开发出的微型计算机的技术才能使微型机成为无防备的富源。

IBM的个人计算机是为可存取性和使用方便而设计的。它采用的是小规模组织和易更换的硬件部件，而功能强，可靠性高并可携带。与它的祖先，中大型计算机和小型计算机相比，微型机极其便宜，操作迅速，数据的复制和传输精确无误。就个人机设计而言，存在的问题正是安全问题。

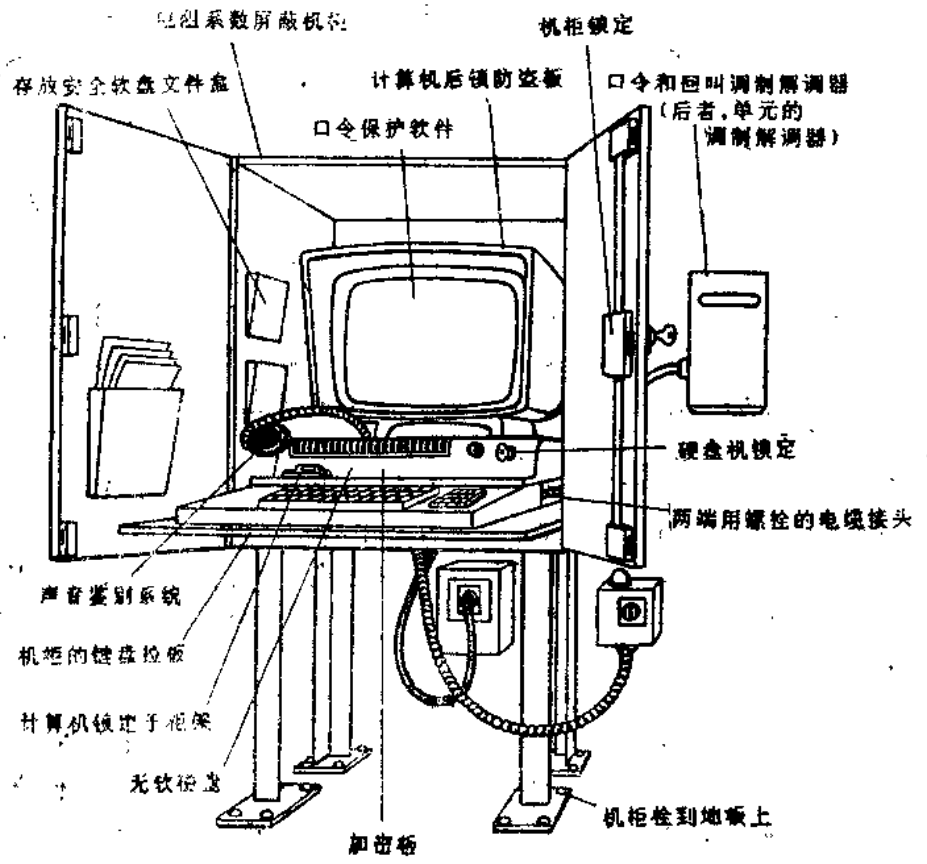

图 1.3 具备安全保护的个人计算机

在这种情况下，似乎要用技术来解决微型机的安全问题。这如同火来灭火，是错误的。技术并不是万应药，它只是助手，并不会解决问题的根本。

多少年来，技术使得复杂的硬件比以往更为严密，更为可靠。但是，同样也是这技术给对手提供了方便，使之能便宜地购到高速处理设备，并且用计算机来发掘其他系统

中的薄弱之处。由于技术越加复杂化，世界上其他地方那些初露头角的计算机罪犯所得到的教育也较为良好。

对技术的信仰很容易变得盲目起来。可能是因对技术领域引出的一些特别问题的忧虑，我们变得蛊惑起来了。然而，这种信仰会混淆原有较准确的判断。从一个计算机罪犯的坦白中看出，世界上所有的技术都不会使他受挫。他们会像掠夺者那样，搜寻出最虚弱的环节，就象盔甲上的裂口。要想在自己的计算机系统上封住每一个极小的开裂点都得花费巨大的代价。尽管这样，大胆的窃贼们仍将能找出办法闯入的。

微型机系统牵连的人多于机器设备。技术将永不会取代人的因素。技术人员能使计算机运行，也许安全产品更有效些，但是，如果操作人员或是用户失职——滥用契约职责——这点技术能解决吗？技术好似一只裂着大嘴在侧道上等候着的野兽。

传统上，安全一直是那些技术专家的领地，闹哄哄地主导这个，改进那个。但十分有趣的是，从几乎所有记载的计算机犯罪案例中得出了截然不同的结论：每个现场都具有对犯罪起技术保护的措施，可都没有生效，为什么呢？那又是什么因素在起作用呢？是什么控制失效了呢？这些以及相类似的问题将在书中进行研究探讨。

六、与计算机有关的犯罪

作为反派角色的计算机已成为科学小说中受人欢迎的主题，而今计算机反派角色已成为大众眼里的民间英雄——罗宾汉或布莱克巴特绅士。计算机犯罪或计算机罪犯到底有什么与众不同之处？

计算机增强了人类的智能，就像机器放大人类的骨骼一样。它扩展了智力的距离和边境。计算机效力高、精确、明断、无情、无生命。普通大众私下都害怕计算机，要利用计算机（神话般的东西），那计算机罪犯必须具有最高级的狡诈，即才能和勇气——所有那种非常浪漫和带有个人主义色彩的气质一定具有捕获普通人想象力的魅力。

让我们从现实的高度出发研究其本质。计算机罪犯同其他罪犯一样，是一个一心想得利的机会主义者，从惩罚角度来讲，计算机犯罪并不是独特的犯罪形式，但却是所有犯罪的一种折衷变形。计算机犯罪由传统的犯罪形式组成——欺骗、偷窃、非法侵占财产、贪污、破坏、纵火及敲诈。计算机本身却成了无意同犯或是犯罪的牺牲品。

与计算机有关的犯罪仅是计算机安全戏剧中的一个角色而已，但是一个重要角色。从1965年以来，仅以报导的一千多个计算机犯罪案例来计算，共损失了成百上千亿美元。在这其中还有一个较大的差异，即确切的损失与报导的损失之比。谁也无法知道就在官方的鼻子底下究竟发生了多少案例。尽管这是逐步变化的，但公司还不愿证实这反面宣传冲击所致的恐惧。公司的策略是强调从容的形象。一份近期《计算机世界》评述阐明了这一特点。两百家大公司被匿名质问，约30%左右（约60家公司）坦白是计算机犯罪的牺牲品。60家公司中至少有40家公司断定他们知道犯罪者，是内部的自己人所作的案。公布于众以后，响应者才估计每次作案平均损失额为1000万至1500万美元。根据发现的情况表明，没有一个犯罪者被起诉。

计算机在犯罪中所扮的四种角色

（1）客体——破坏计算机、数据或是程序。拆毁操作计算机必备的设施和资源，

如电源等。

（2）主体——现场或环境的计算机犯罪。

（3）工具——计算机作为复杂犯罪活动中的抵押品或工具。计算机可能成为犯罪中的一个得力助手。如用于扫描译解、口令字码的电话编码，企图占用未经批准的电话。在欺骗阴谋中，计算机可能是被动的工具，被骗于编好的程序而发给不在册雇员工资。

（4）表征——计算机被用于欺骗或恐吓。如类似某些计算机算命服务来骗取牺牲品金钱的假广告阴谋。

微型计算机犯罪的潜在力是令人惊愕的。个人计算机分散于各个组织内。存贮介质（软盘、固定硬盘和盒式磁带）体积小，并易于隐蔽。个人计算机是无掩蔽式的，它的操作系统是个玻璃结构，缺乏任何存取控制。高度机密的数据会被诱惑到盗窃者手中。个人计算机重量轻而且紧凑，能随身携带。

人们，特别是刚刚接触微型计算机技术的人倾向于绝对相信计算机。他们有这样一个幻觉，认为计算机从不说谎。任何用计算机打印在纸上的数字看来都是官方的，一定是精确的。审计员很早就发现了一件可笑的事，手写文件立即被猜疑，而打印的同一文件却通过了真假检验测试。

七、与用户友好意味着与滥用者友好

当用户埋怨软件程序太不易看懂时，软件发表者就迅速援助。这样就开始了用户友好软件时代，也是因此导出了一个微机安全的恐怖故事。无思维任务软件最易进行无思维数据曝窃或数据欺骗。为了不正当数据欺骗涉及到增加薪水或得利率而对数据故意改动。令人啼笑皆非的是"欺骗"这词是愚蠢的、冒名顶替之意。然而，数据欺骗则是难以防护的数据犯罪，是潜在的最大破坏。数据欺骗者也许觉得审改医疗记录，任性地更改血型很有趣。但是，输进异型血的无辜牺牲者并不会与他一样觉得有趣。

伴有屏幕提示而装入菜单式驱动的有用程序专门设计成手把手地教用户操作，它可以让用户慢慢地，一步步地使用所有程序。程序不会区别他是合法的用户还是卑鄙的人，将会同样地让卑鄙的人进入极其重要信息的保密室。

软件发表者重申："如果你将要犯错误，是在用户的支持下犯错误，那么属于安全范畴"。这条不成文的法律来挡开外来的抨击。完全的可靠性自始至终要有安全来作为基础的基础。现在用户们比以往更加精通计算机。本人感到奇怪的是，是否软件发表者低估了微型机用户的智力和不断增强的才能。

八、计算机罪犯的传略

由于社会在变化，为此犯罪的情况也同样在变化。多数由于技术、教育和微型计算机的进步，我们处于第二代计算机罪犯的时期。自从十九世纪有了公路强盗以来，我们已经历了百年的历史。事实上，计算机罪犯是个较为年轻的专家治国论者式的罪犯——白衣领，无衣领，以及分散的青少年。有多少学校的教学大纲向年轻人提供个人机，有些甚至还在幼儿园呢？许多小孩不会阅读前就学着在计算机键盘上打字。向青少年介绍

一种新的Siliconese语言，这名字已被收进现代俚语之中。青少年在破坏计算机的挑战中受到了同类人的鼓励……现代新型男子气概。《个人机》杂志和不定期公报登出了有关对薄弱系统软件藐视的见闻，并训练自愿者和积极分子破坏大多数数据库的方法。

这些日子里计算机罪犯持续不断出现，他们以询问方式始终注意着袭击系统的机会。这些日子里，引人注目的行窃者却不是微型机风险经理必须提防的主要罪犯。防止个人机受行窃者的破坏是一种相当简单的事情。专业罪犯则是最大的威胁。计算机专业人员是另一类人。

专业人员不像通常的行窃者，不是挤进来的人，他们也没有时间为破坏口令去执行多余的试错扫描。专业人员要的是进出速度快，专业人员窃听者在进入计算机RAM（随机存取存贮器）内存贮时，就能在你的个人机上装上器件，记录下击键数或是窃听电子脉冲（类似从电话线路上窃听情报）。

当然，行窃者确实有他们自己的社会等级，但许多人的技术奇才还应该像管理枪支一样经官方正式鉴定。

计算机犯罪是类似其他犯罪的一种弊病。对于寻机作案的罪犯来讲，一旦发现系统的窥孔或秘密途径再放弃这种行动是极其困难的。无论什么激发了他，是猫与鼠的恐怖小说或只是十足的贪心，最终都会征服他，也绝不会放手。当然，他不认为在伤害任何人，计算机是一个抽象的不存在的东西。甚至，他认为自己仅是在跟系统打交道，仅此而已。

或者说，抢劫富人来供给穷人——他自己。

第二章 硬件盗窃

一、防止硬件盗窃

两台或更多的个人机集合在一起，窃者必定会跟随而来……**除非补充和加强控制功能。**

一个成功的窃者总有他有机可乘之处。未加控制和分散的个人机都必须加以紧密控制和联系。物理上的控制越少，作案的机会就越多。

两种类型的罪犯涉猎硬件盗窃：窃贼或外人，内部或雇员小偷。重视这一点，然后再看以下的统计数会使一些人瞠目吃惊：

·根据美国联邦调查局的相同犯罪报告处的统计数，1980年价值9400多万美元的办公设备被偷，在过去的五年里，此统计数呈稳定上升趋势。

·在任何地方均有5%至75%的雇员在本公司内偷窃。有10%至30%的雇员连贯地从事盗窃。目前有25%至80%的雇员常在无安全防护措施的地方进行偷窃。

·窃贼有他们的类型体系。

业余窃贼是个机会主义者，70%以上的窃贼属于这一类型。28%的窃贼是半专业性的，这对商业界形成了最严重的威胁。他们有转让和处理掉赃物的手段。仅2%的窃贼是专业性的罪犯，这些人能击败最复杂的安全系统。

·做小生意的人受害最大。有85%的小商业因遭到罪犯的偷窃损失商业收入额比其他商业损失高出23倍，总额超过500万美元。

·在全国范围内，6件盗窃案仅有1件能破获。

假如系统安全仅仅就这些的话，那么系统不仅值得窃贼来偷，而且已成为疯狂者从事破坏的诱人目标。计算机还受到多种形式的破坏，如被枪射击，被汽油或燃烧瓶烧着，被可塑炸药轰炸，被螺丝刀戳坏，从窗口被抛出或被掷向墙壁以及受妇女鞋跟的袭击。

二、地下市场的需求

计算机窃贼几乎会获取任何他能控制的功能性设备，这对他来说并不独特。出售微型机、外设、计算机内部组件、个人机装置、存贮介质的黑市场正在惊人地发展。目前盛行的计算机旧货物交易会招来各类罪犯和那些相似的交易寻觅者。窃贼掠夺计算机就象偷窃汽车一样，来自各种窃贼的威胁和压制，作出判决越来越困难，计算机的市场价天天在上升。供求规律也只在社会的边缘实施。任何人仍能花零售价格中的一部分钱获得一台畅销的计算机。

不必提醒公司在计算机设备上的资本投资，这是微不足道的，但设备应该受到保护。尽管硬件价格是动态的，但为了买一台香子兰机器还是支付了2000美元至4500美元，或由于个人机配置高级，支付的钱就更多。

所有计算机设备都应该标上去不掉的顺序号。计算机窃贼最初采取的行动之一是扯掉通常贴在计算机或外设后盖上的顺序号码板。他们只需化不到5美元购买一把金钢钻刀刃的雕刻刀，就可把自己公司的名字以及顺序号直接雕在机器上。万一被地方警察部发现被盗的设备，则可见的顺序号就是唯一的证明。

当系统被盗，承担的损失远远大于最初的硬件代价。更多包括在内的是替换费用；必须计算生产上的损失及雇员的工时。或许被盗的是具有固定盘的系统，但比这损失更多的则是失去了有价值的程序和数据，除非严谨地制作过后备复制品，否则必须再生成这些信息，那就需要时间。当然，这些都是由于盗窃所引起的与时间有关的代价，即清算残骸，估价损失额。如果计算一下办理保险索取（如果已经保险过的设备），报告警察所化的时间及投入的时间和精力就可买到一个新系统。

惊奇地发现，竟有这么大批经理不能真正确切地说出公司的办公室里有多少台个人机在运转。基本的防盗安全措施是列出详细的个人机财产清单和绘出办公室的确切位置图。如果一个办公室里有一台以上的个人机，那么其区域应要清楚地表示出来。一个区域可能有两台紧靠着的个人机组成，也许所表示的办公区域（公司内的一个部门）安装了一组个人机。作为一个经理不仅要为各个人机位置提供文件，并且要为各台个人机配置中的所有组件和外设、个人机的指定用户、以及为这些用户的应用处理提供文件。

下面举例的查收清单供制表者作参考：

表2.1 个人机财产清单

计算机 #1：	编号 #：	位置：
键盘：	编号 #：	用户#1： 作业：
显示终端：	编号 #：	用户#2： 作业：
打印机：	编号 #：	用户#3： 作业：
键盘：		用户#4： 作业：
#1 #2		用户#5： 作业：
#3 #4		用户#6： 作业：
#5 #6		
其他存货		

如果买进的个人机超过一台，聪明人应绘制出各台个人机的工作平面图，标出其物理位置，越完整越好，指明个人机的所有用户，用铅笔点出通路和出口处。由于个人机的配置会扩大，应相应调整布局。

一句忠告：要保存好所有的安全信息，比如要锁好清单，否则将使窃贼很方便地获得设备的位置连同公司财富的精确示意图。

三、侵入报警

预防侵入是保护任何昂贵商用设备的基本措施，但对计算机来说并不是唯一的措施。门窗上报警器的声响可迫使侵入者离开目的地。大型计算机的安装配备了多级保

此为试读，需要完整PDF请访问：www.ertongbook.com