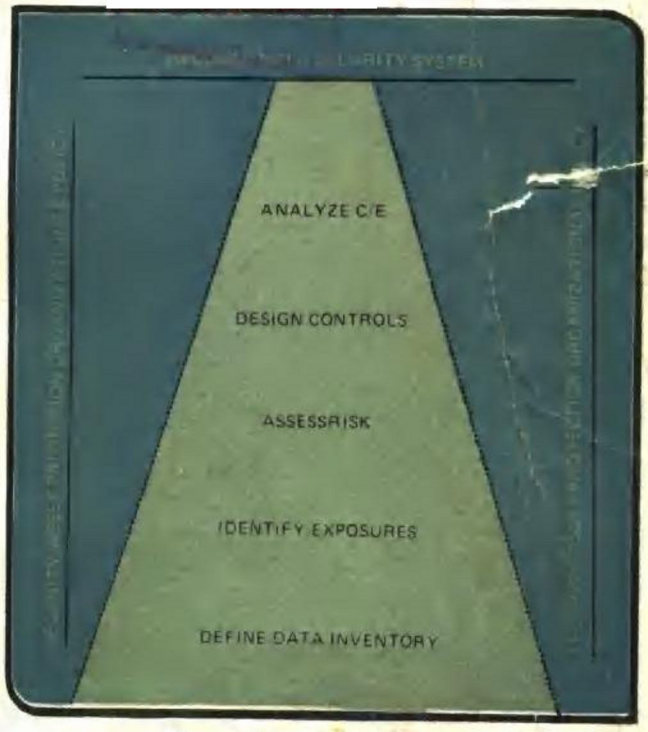
信息系统的安全保密

美 R. P. 费希尔 著

INFORMATION SYSTEMS SECURITY



科 学 出 版 社

信息系统的安全保密

〔美〕R。P。费希尔 著

张连超 张盛英 译

科 学 出 版 社

1987

内 容 简 介

本书论述了计算机系统数据安全保密问题。全书共十二章，前四章说明信息系统安全保密的必要性、关键问题、安全系统的一般功能和管理人员的基本职责。其余各章系统地介绍怎样识别、分析各种数据危害，如何选择效费比合算的控制措施，以保障计算机系统数据的安全。原书有六个附录，是IBM公司等单位关于数据安全保密事项的具体规定。此外，译者还增选了美国国防部的《工业安全保密手册》和《情报资料保密条例》中相关的章节，以供读者全面参考。

本书通俗易懂，适合信息系统、计算机用户、保密保安部门的管理和研究人员，以及对信息安全保密感兴趣的人员阅读。

Royal P. Fisher

INFORMATION SYSTEMS SECURITY

Prentice-Hall, Inc., Englewood Cliffs, N.J., 1984

信息系统的安全保密

〔美〕R. P. 费希尔 著

张连超 张盛英 译

责任编辑 李崇惠

科学出版社出版

北京朝阳门内大街137号

中国科学院印刷厂 印刷

新华书店北京发行所发行 各地新华书店经售

1987年12月第 一 版 开本：787×1092 1/32

1987年12月第一次印刷 印张：10 3/8

印数：0001—3,200 字数：231,000

ISBN 7-03-000111-7/Z·4

统一书号：15031·892

定价：2.45元

译 者 前 言

如果说，几百年前培根的名言“知识就是力量”已为举世公认，那么，我们今天就完全可以断言：“信息就是力量！”因为就其实质来说，信息就是知识。当然，确切点说，信息是指“用特殊关系得到的在某一方面所必需的知识”，或者是指“为了根据情况而作适当的判断并采取行动所必需的知识”。在信息论中，信息是指“用符号传送的、对接受者来说预先不知道的知识内容”。尽管“信息”一词很抽象，难以准确定义，但信息的实体是知识这一点是比较明确的。

作为现象、概念、思想和决定等等的反映，作为人类社会活动所必需的知识，信息可以说是无所不在、无处不用的。无论是生产经营还是日常生活，一时一刻都离不开信息。尤其是处于当今人类正在从工业化社会向“信息社会”过渡的时代，信息的作用就更为突出，成了影响社会发展的关键因素之一，它同物质和能量一起，被并称为“现代社会的三大资源”。物质和能量这两项“基本资源”的重要性是显而易见的，但若只有它们而没有“信息资源”的配合，任何生产结构或社会组织都不可能发挥应有的功能，甚至难以为继。现代科学管理的主要任务之一，就是掌握和利用信息。例如企业管理，就是企业领导利用它所掌握的“信息资源”，对企业所拥有的资金、人员、设备和材料等“基本资源”进行统一规划，合理支配。在行业竞争中，谁能及时、准确地掌握行情变化（市场信息），因势利导，随机应变，谁就能占领市场。因掌握了关键信息而获得成功，反之因泄露了核心机密而招

致失败的事例，不论是在商业情报战还是在军事情报战中，都是屡见不鲜的。鉴于信息特别是敏感信息，对国家、团体或个人的重要价值，竞争或对抗的双方，总是千方百计地攫取对手的机密信息，而同时又总是小心谨慎地保护自己的重要信息。

信息的作用在当今社会交往中之所以如此重大，是因为得力于它的处理手段——电子计算机的迅速发展和广泛应用。以电子计算机为主体的现代信息系统，是“信息社会”的根本标志。目前，各国都在竞相发展信息技术，改进信息系统。在这方面，保密与窃密的斗争是十分激烈的。难怪，在美国为限制出口而编制的“关键军用技术清单”上，信息系统被列为十九类关键技术之首，成为最重要的保护对象。

总之，在科学技术日新月异、社会活动纷繁复杂的时代，信息成了事业发展不可缺少的资源，处理信息的计算机成为现代管理最有力的工具。由信息及其处理工具构成的信息系统，正在改变着社会的经营组织和管理体制，改变着人们的劳动习惯和生活方式，促使世界环境发生深刻的变革。

但是，任何事物都有它另外的一面，计算机信息系统的广泛应用，也会给社会增添某些问题。信息（数据）在收集、存储、处理、传递、显示和使用等过程中的安全保密便是主要问题之一。计算机不管如何神通广大，都离不开人的管理。管得好，它为你造福；管得不好，也会给你肇祸。在国外，有人利用计算机本身设计上的缺陷，或者利用管理工作上的漏洞，投机取巧，营私舞弊，非法泄露、改变或损坏系统中的数据，这就侵害了系统的完整性。人们把利用计算机“捣鬼”称为“计算机犯罪”（或叫“智能性犯罪”）。有关计算机作案致使某公司或某银行损失多少多少的标题，不时见

诸报端，从而唤起人们对信息系统保密保安问题的密切关注。的确，随着现代信息系统的结构日益复杂和应用日益广泛，系统的保密性、安全性和可靠性问题也日益明显和重要。许多人认为，计算机系统的安全保密问题，是当今计算机科学实际应用方面的最关键的问题之一。这一问题不解决，系统的理想状况就无法达到。因此，研究这一问题的著作也就应运而生，并且逐渐增多。《信息系统的安全保密》一书便是其中之一。

本书作者是美国 IBM 公司信息系统管理研究所的高级研究员。他长期以来专门从事信息系统管理和控制的研究，大力宣传计算机系统的数据安全保密问题（为此，不仅在美国国内授课，还到欧洲、亚洲和大洋洲等地讲学）。本书便是他多年研究工作的经验总结。其特点是：

1．抓住普遍存在的关键问题。作者根据以往的管理实践所列举出的十八个关键性控制问题，对所有计算机信息系统来说，都是有可能出现的，必须加以密切关注；他所论述的数据保护的原理和方法，也是最基本的，对现有系统和新设计的系统一概都适用。

2．强调管理人员的控制作用。书中反复说明"安全保密人人有责"，而且职责要具体分工要明确，管理部门必须负责制订这方面的计划与规章。附录中的 IBM 公司的文件，详细规定了各类有关人员（经理、数据所有人、用户和保管者）在保护数据财产上应负的责任。

3．注重常规的安全措施。全书本着讲求经济效益的观点，提倡利用简单易行、事半功倍的控制手段（如责职划分和保密教育等），而不主张一味追求搞什么新奇奥妙、费用高昂的检测设备，强调要进行效费比分析，以便选择价廉物美的控制装置。这对经济、技术力量较弱的单位来说，尤为

重要可取。

正如“序言”所说，本书在计算机信息系统安全保密方面，也许是“头一部”著作，而且是“非技术性的”，所以对许多问题只是作一般性的论述，没有进行技术上的深入探讨，因而不可能完全满足某些专业人员的需求。

随着我国信息技术的迅速发展，计算机的广泛应用，以及企业间相互竞争的出现和加强，信息（或数据）的安全保密问题，必然会提到有关部门的议事日程上来。出于这种考虑，特将这本概述这一问题的基本读物，推荐给设计、使用和管理信息系统的人员，以及对信息保密感兴趣的读者。

本书在翻译过程中，部分章节得到曾民族研究员、罗光夏副研究员等同志的热情帮助，在此谨致谢意。

由于译者水平有限，译文差错之处在所难免，敬请读者指正。

译　者

序　言

本书的梗概

在计算机信息系统安全保密方面，本书也许是“头一部”著作，其内容是介绍有关保障数据安全的一套简单有效、系统完整的方法。同样重要或许更为重要的是，本书指导人们在为此项工作投入人财物等资源之前应集中关注什么问题，也就是说，为保障信息系统的安全，使危险限于可接受的程度，人们可直接采取哪些效费比合算的措施。

是非技术性著作

本书在叙述数据安全保密时，力求不用太专的技术语言，也不详细讨论数据安全保密领域中每个问题（诸如数据库、通行字或职能机构）的具体方案，而是提出构思或方法，目的在于有效地解决数据安全的主要问题。关于如何看待和解决自动信息系统中当前存在的数据安全保密问题，本书提出了几种主张。书中还概述了在制订数据安全保密计划之前所要考虑的各种因素，这对读者也很有益处。

首先应关注什么问题

数据安全保密要考虑哪些关键问题，而为解决这些问题，安全系统又应具有哪些基本原理、特性和功能？此外，在数据安全保密工作的计划、实施和管理过程中，管理人员起什么作用，承担什么职责？本书第一章至第四章便要阐述这些问题；作者认为，在动用人财物等资源去解决信息系统

的具体安全方法问题时，这些问题需要首先加以解决。因此，开始这四章对信息系统行之有效的安全保密做法，作了概括的叙述。

第一章：公司管理部门优先考虑的问题

对一个单位来说，数据安全保密真是一件具有重大意义的事情吗？如果是，那又为什么？要说在当今信息系统中缺乏足够的控制措施，有证据吗？究竟需要采取什么措施？如何确定本单位是否有必要提高数据保密的程度？而第一章则指出了为什么现有的许多计算机信息系统，缺乏足够的安全措施。这一章还附有一些简单的供自我评定用的测验题，以衡量你们单位的管理部门，对数据安全保密的主要问题和利害关系还需要给予多大的关注。

第二章：控制措施的关键问题

对过去设计的信息系统来说，适当控制的关键因素是什么？管理者、检查者、设计者和关心数据安全的其他人员，应把注意力放在哪里，人财物等资源应集中用到什么地方？第二章提示读者，应该首先着眼何处。这一章论述虽然肤浅（因为每个问题均可深入写成一本书），但它确实阐明了每个关键因素的性质，有助于读者掌握有待解决的问题。

第三章：系统的原理、特性与功能

对数据安全保密感兴趣的人来说，在安全系统方面，有哪些基本原理、特性和功能，可供借鉴、利用？通常行之有效的安全方法是什么？第三章简单明了地介绍了 IBM（国际商业机器公司）和其他公司认为对信息系统安全保密颇为适用的许多设想、概念与技术，并且通俗易懂地评述了某些业

关系。这几章还利用科学分析方法，就系统安全保密措施的选用问题，向管理人员提出效费比合算的建议。

第五章：危害的判定

第五章一开始就说明“危害”和“数据安全”的定义。根据这些定义，人们可采用简单的方法检查各种违章举动（不样之兆）对数据产生的结果或后果。由各种对数据不利的行动，即无意和（或）有意的泄露、改变和损坏所产生的危害，基本上分为六类。接着说明导致数据危害的基本起因，以缩小判定过程的范围，最后提出下一章将要讲述的产生数据危害的环节，从而为判定信息系统的危害提供了井井有条的思索方法。

第六章：危害的控制环节

第六章讲述判定危害的方法所涉及的范围——数据危害发生的全过程，整个过程包括十一个离散的控制环节。

第七章：方法论的应用

本章用图解方法说明，如何结合数据处理过程的十一个基本控制环节，把判定危害的系统思索方法，直接应用于某一信息系统（如工资管理系统）。

第八章：减少危险的方法

怎样才能使危险降到最低程度？采取什么基本步骤去减少危险？第八章向系统设计者深入地说明，在所有信息系统中，大体上应怎样才可减少危险，它提出了安全控制的某些基本指导原则。如果人们对危险进行定量分析，那么，这些指导原则便有助于使信息系统获得成功（使危险降至最低限度）。

已公布的安全设计理想方案的基本内容。而对那些不熟悉数据安全保密问题的人来说，读了这一章便会明白什么做法可以参考。

第四章：管理人员的重大作用

第一部分：管理的策略、计划与规程　在数据安全保密方面，管理人员起什么作用？第一部分说明，管理人员有必要为数据安全保密工作制订适当的策略、计划与规程，并结合附录中的参考实例，具体描述它们的形式、内容和用法。其中还指出，要使数据安全保密工作卓有成效，还必须发挥信息系统本身之外的管理人员的作用。

第二部分：安全保密管理员的作用　数据安全保密工作是谁的职责？安全保密管理员应具有什么样的特点与能力？为了管理好数据资源的安全保密工作，必须建立负责这类工作的职能机构。最好借助于职责一览表来反映这类工作的责任。小单位、小系统可能不派专职人员承担这类任务，但必须认识到确有必要这样做。

方　法　论

关于安全保密问题，已经见到过许多极好的文章。但是，其中提出的许多见解，至今尚未综合成井然有序、简单明了的方法。做实际工作的人，总是需要详细的指导材料或“须知”手册，以便进行数据安全的设计与控制工作。而检查人员，则一直在寻求简单有效的手段，以便对业务上的控制措施作出适当的评价。第五章至第十一章所列举的方法，有助于满足这两种基本需求。这七章是本书的主旨所在；它们向读者揭示，如何通过数据处理全过程，即十一个界限明确、可以掌管的控制环节，来综合考察数据安全保密的所有利害

第九章：危险分析

第九章为实际工作者提供一种分析方法，用以定量说明同每种特定危害有关的危险程度。这种定量研究可以做得极其严密。但是，必须注意：定量分析方法要适当，其花费不应超过预期的危险会带来的损失。怎样才算适当，最好按照常情衡量。

第十章：基本控制措施

这一章提出一种选用控制措施的独特方法，以便简化这种选择过程。通过综合考察数据处理过程中的软件控制措施，便可看到它们的适用范围。某种控制装置一经选定，对其费用和有关的成功概率，就要加以测定和记录。本章还列有控制装置登记表，以供参考。

第十一章：效费比的选定过程

第十一章运用投资报酬率（ROI）的概念，对推断出的危险和控制费用的定量数值，作了分析研究。外界可能会强求采用某些效费比不佳的控制措施。但最终要根据预定的危险值容许限度，来选择适当的控制装置。

捷　径

第十二章：捷径

最后一章简捷地概括了五至十一章介绍的系统的方法。这种“捷径”采用与前几章相同的方法，只是简化了严密的定量化过程。它所反映的只是安全保密的大概面貌，而不是详细情况。掌握了概貌，那就便于对控制措施作出总的估价。而站得高，看得远，系统的弱点也就容易发现。如果对

系统安全保密问题只拟作些走马看花似的粗略观察，那么本章提供的“捷径”便是最有效的手段。

如何阅读本书

作者建议，为了解全书的大致内容，首先应通览一下全书；然后可按各自的兴趣与需要，重点细读专门章节。希望本书内容将起到抛砖引玉的作用，推动读者去创立并实施一种更好的方法。在为当今信息系统寻求更加有效的保密保安途径方面，大量工作正在进行，本书只是其中一个部分。

作者致谢

我要特别感谢IBM公司数据安全计划主任威廉H.默里(William H.Murray)，他对本书若干章节的撰写给予了巨大帮助。本书数据安全保密的总体构思，体现了他著作中许多基本观点。

另外，承蒙IBM公司准许，本书选录了该公司几份有关数据安全保密问题的文件，作者对此深表感激。IBM公司的文件以及其他数据安全专家的几份资料，已作为附录收入本书。

罗亚尔P。费希尔

目　录

第一章　公司管理部门优先考虑的问题

优　先　程　度

公司企业的发展壮大、繁荣昌盛，有赖于其上层管理部门的正确领导。公司领导的关键职责，一向在于筹划和利用本身的各种资源，即传统所说的那几个大“M”：Men（人员）、Money（资金）、Material（原料）和 Machines-and-facilities（机器与设备等固定资产）。

随着电子计算机的问世，又出现了一种需要公司上层管理部门密切关注的新资源，这不是计算机本身，而是计算机处理的信息的组成部分——**数据**！

管理人员迟迟才认识到数据也是一种重要资源。如果单独地看，零散的数据似乎既没什么意义，也无多大危害。但把已建成的数据库作为一个整体来看，数据便可成为业务工作最关键的资本之一。数据何以如此宝贵？答案就在于它对那些占有者或需要者来说是有价值的。他们承认信息就是力量——管理的力量，操纵的力量，支配的力量。至于数据价值的大小，通常直接取决于它改变或影响人们行为的程度如何。

计算机及其有关存储手段，确能使管理部门获得所需的信息。但是，管理部门对于如何保管好获取信息所用的手段这一问题，并非总是那么重视，并给以优先考虑。

在许多公司企业中，电子数据收发系统现已广泛使用。可是在这些系统的开发与实际应用过程中，多数还缺少或者说根本就没有管理部门的参与和指导。控制措施不仅很不得

力，而且简直可以说就没有。在目前新建的某些系统中，这种状态同样存在。

目前对信息系统缺乏控制，原因也许是，数据处理部门、检查部门或其他管理保障部门，还未强调或宣传控制的必要性。另一个原因可能是，计算机厂商在设计上往往偏重于简单方便，而不太愿意复杂麻烦。此外，管理人员恐怕也有一定责任，因为他们没有及时把保管计算机信息系统这件事，真正列为自己的一项新的职责。

促 进 因 素

促使管理部门关注信息系统安全保密的因素主要有两个。一是由计算机管理上的漏洞引起的“衡准基金”*问题。虽然报上把它宣扬为“计算机犯罪”事件，但事件中的弄虚作假、营私舞弊，与计算机本身并无多大关系。然而，报上“损失2,725万美元”的醒目标题却引起了上层管理人员的重视，他们开始意识到在数据安全保密方面自己应负的责任（也就是说，必须采取措施去保护信息，未经许可，任何人不得有意或无意地加以泄露、改变或损坏）。遗憾的是，管理人员由于没有继续关心、深入考虑这个问题，所以安全保密观念不久便淡薄了。

引起管理人员关心数据安全保密的第二个主要因素便是《1977年对外行贿行为法》(The Foreign Corrupt Practices Act)，现称《商业惯例记录法》(The Bussiness Practices and Records Act) 的颁布。其条款对国内任何公办的公司均有影响。国会颁布的这项法律，原是为了阻止美国

---

* 衡准基金 (Equity Fanding) 系为补偿银行透支而发行的长期债券。——译者

公司向国外贪官污吏私送非分钱财（商业行贿）；后经证券交易委员会（SEC）裁定，扩大其效力，据以要求公司管理人员在他们的财务报告中，说明安全保密措施是否得当，作用是否理想。

该法修订了《1934年证券交易法》的条款，明确规定了一项强制性要求，即公司必须实行内部会计控制制度，以便实现下列四项目标[1]：

1．商务活动要依照管理人员一般的或具体的授权进行。

2．商务活动要适当备案，以便

(a) 能够依照通行的会计原则准备财务报告；

(b) 保持资产帐目清楚、可查。

3．只有根据管理人员一般的或具体的授权，方可动用资产。

4．每隔一定时间，要将帐面资产同实际资产进行核对，发现任何差错，就要采取适当措施。

另外，该法还规定，每个公司必须根据要求说明，它：

1．评价了管理制度的现状；

2．弥补了管理制度上的所有缺陷；

3．继续在监视这种管理制度的实际效能。

如违背上述法规，公司负责人可被处以五年监禁，或1万美元罚款，甚至既坐牢又破财。这就再一次促进管理人员，把计算机信息系统的安全保密工作，列为自己主要关注的问题之一。公司领导一重视，这项工作立即见效：建立起EDP（电子数据处理）检查机构，委派了数据财产保管人员，并初步制订有关信息系统安全保密的专门策略、计划和

[1] The American Institute of Certified Public Accounts(AICPA) Statement on Auditing Standards.