信息安全管理概论

——BS7799 理解与实施

科飞管理咨询公司　编著

机 械 工 业 出 版 社

本书从BS7799(ISO/IEC17799)信息安全管理标准入手，全面系统地介绍了现代信息安全管理的思想与方法，以及企业信息安全管理认证。全书共分6章，第1章信息安全管理概述，主要介绍了信息安全现状、信息安全概念及信息安全管理模型；第2章信息安全风险评估与管理，系统阐述了风险评估与风险控制的方法；第3章风险管理惯例，提供了可供不同组织选择的安全控制方法，并介绍了有关信息安全的专业术语，如访问控制、身份鉴别、数字签名、信息验证等；第4章信息安全管理标准，主要对建立信息安全管理体系的所依据的BS7799-2标准进行了诠释；第5章介绍了建立信息安全管理体系的方法与步骤，为组织建立并实施信息安全管理体系提供了指南；第6章信息安全管理体系认证，介绍体系认证的基本知识与体系认证的过程。附录列出了与信息安全有关的法律法规，以供读者参考。

图书在版编目(CIP)数据

信息安全管理概论——BS7799理解与实施/科飞管理咨询公司编著. —北京：机械工业出版社，2002.4
ISBN 7-111-10130-8

Ⅰ.信… Ⅱ.科… Ⅲ.信息管理—安全技术
Ⅳ.G203

中国版本图书馆CIP数据核字(2002)第019607号

机械工业出版社(北京市百万庄大街22号 邮政编码100037)
责任编辑：常淑茶 版式设计：霍永明
封面设计：鞠 杨 责任印制：付方敏
北京铭成印刷有限公司印刷·新华书店北京发行所发行
2002年4月第1版·第1次印刷
890mm×1240mm A5 8.125印张·238千字
0 001—4 000册
定价：21.00元

《信息安全管理概论》编写组

组长　　门洪利

主编　　孙洪涛　门洪利

编委　　俎全胜　王毅刚　于海霞　吴昌伦

前　言

现代企业对信息的依赖越来越大，没有各种信息的支持，企业就不能生存和发展。信息已成为现代企业的一种重要资产，需要加以妥善保护，否则，可能由于人员(疏忽、跳槽、破坏)、竞争对手(商业间谍、收买、盗窃、网络攻击)、设备故障、系统缺陷和灾害(爆炸、雷击、火灾、地震)等原因，在一瞬间信息资产被毁灭、消失、损坏、盗窃、贬值、转移，给企业带来致命的打击。由于计算机、通信、网络等现代化技术的普及应用和人员流动的频繁，信息受到的威胁更大。为了国家、企业和个人的信息安全，加强信息安全管理刻不容缓！

目前，我国的信息安全管理主要依靠传统的管理方式与技术手段来实现，传统的管理模式缺乏现代的系统管理思想，而技术手段又有其局限性。保护信息安全，国际公认的、最有效的方式是采用系统的方法(管理＋技术)，即确定信息安全管理方针和范围，在风险分析的基础上选择适宜的控制目标与控制方式来进行控制，制定商务持续性计划，建立并实施信息安全管理体系。这种系统的信息安全管理方法已经成为国际性标准 ISO/IEC17799(BS7799)。

如果到书店里逛一逛，就会发现关于网络安全技术的书籍琳琅满目，但关于信息安全管理方面的书籍很难寻觅。为向广大的信息安全管理者全面系统地介绍现代信息

安全管理的思想与方法，作者根据 ISO/IEC17799 (BS7799)信息安全管理标准，并结合对企业信息安全管理认证咨询的实际经验，编写了此书。全书共分 6 章。第 1 章信息安全管理概述，主要介绍了信息安全现状、信息安全概念及信息安全管理模型。第 2 章信息安全风险评估与管理，系统阐述了风险评估与风险控制的方法。第 3 章风险管理惯例，提供了可供不同组织选择的安全控制方法，并对有关信息安全的专业术语如访问控制、身份鉴别、数字签名、信息验证等进行了解释。第 4 章信息安全管理标准介绍，主要对建立信息安全管理体系所依据的 BS7799-2 标准进行了诠释。第 5 章建立信息安全管理体系的方法与步骤，为组织建立并实施信息安全管理体系提供了指南。第 6 章信息安全管理体系认证，介绍体系认证的基本知识与体系认证的过程。附录列出了与信息安全有关的法律法规供读者参考。

本书面向包括企事业单位、政府组织的信息安全管理人员与信息安全技术人员。在当今的信息化时代，人们进行证券投资、在家里上网冲浪、刷卡消费等活动已经很普遍，每个人都有个人信息安全的问题，如安全使用各种口令，防范计算机病毒，保护个人隐私等。作者相信一般的读者也会从本书获得一些基本的安全知识，有助于保护个人财产的安全。

本书难免有不当之处，欢迎读者批评指正。

科飞管理咨询公司

2002 年 3 月 15 日

目　录

第 1 章　信息安全管理概述

1.1　信息安全管理历史回顾与现状

1.1.1　信息安全管理历史回顾

国际公认的 ISO/IEC IT 安全管理指南(GMITS)对信息(Information)给出如下解释：信息是通过施加于数据上的某些约定，当前赋予这些数据的特定含义。信息可以理解为消息、情报与知识。信息本身是无形的，借助于信息媒体以多种形式存在，有的储存在计算机里，有的保存在磁带或光盘里，有的被摄制在微缩胶卷里，有的记忆在人的大脑里，有的通过网络传送，有的打印或记录在纸上，有的由传真发送传输，通过不同的交谈方式来表达或通过不同的设备显示出来。信息也是一种资产，不仅包括与计算机、网络相关的数据、资料，还包括专利、标准、专有技术、商业档案、文件、图样、统计数据、配方、报价、规章制度、财务数据、工艺、计划、资源配置、管理体系、关键人员等等。信息是人们日常生活、组织正常业务运作和国家管理所不可缺少的资源，无论是对国家、组织，还是个人而言，具有价值的信息资产会面临着各种各样

的安全威胁，因而需要对其进行妥善保护。

信息安全自古以来就是一个人们关注的问题。随着人类文明的发展与进步，信息处理的方法与技术也在不断发展，从最原始的语言交谈，到古代文字、纸张的发明，到现代通信、计算机与网络技术的普遍应用，信息的储存、交流、传输、处理的技术与方法越来越多，越复杂，信息储存的媒体也越来越多。信息量正在呈几何级数增长，信息的传播容量不断增加、传播速度不断加快、信息资产所面临的安全威胁也在不断的增加，因而信息安全技术得到了相应的发展。当然在不同的发展时期，信息安全的侧重点与信息安全的控制方式与手段也不尽相同。

在现代通信工具电报发明以前，信息安全的重点是确保信息的保密性，这包括商业秘密、军事秘密以及个人隐私。信息安全控制方法比较简单，例如采用安全信使传送秘密口信与信件，通过人员的保密意识与物理安全控制的方式来达到信息安全的目的。

电报、电话等现代通信技术的应用，给信息交流提供了极大的便利，这一时期出现了窃听与反窃听技术，信息的完整性得到了人们的普遍重视，如对通信设施的运行维护，以确保通信的畅通与信息传输的质量。

自 20 世纪 40 年代人类发明了计算机，特别是随着网络技术与现代通信技术的飞速发展，信息技术被广泛地应用于各行各业，信息安全已经扩展为对信息的保密性、完整性与可用性全面的保持。为确保信息安全，信息安全技术被许多组织所采用，如加密技术、防病毒技术、访问控制技术等。由于在信息系统设计时注重安全性的考虑，信息处理设施与软件产品的质量与安全性得到了普遍重视，有关信息安全的法律法规、安全技术标准也应运而生。目前，信息安全仍依靠安全技术手段与不成体系的管理规章来实现。在 20 世纪 80 年代末 ISO9000 质量管理标准的出现及随后在全世界广泛被推广应用，系统管理的思想在其他管理领域也被借鉴与采用，如后来的 ISO14000 环境体系管理标准、OHSAS18000 职业安全卫

生管理体系标准，信息安全管理也同样在 20 世纪 90 年代步入了标准化与系统化管理的时代。1995 年英国率先推出了 BS7799 信息安全管理标准，并于 2000 年被国际标准化组织认可为国际标准 ISO/IEC17799 标准，现在该标准已引起许多国家与地区的重视，在一些国家已经被推广与应用，组织贯彻实施该标准可以对信息安全风险进行全面系统的管理，从而实现组织信息安全。

1.1.2　信息安全管理现状

21 世纪具有数字化、网络化和信息化的特征，是一个以网络为核心的信息时代，是一个更加开放与人员流动频繁的时代，任何国家、组织和个人在享受现代技术带来方便、信息共享益处的同时，也面临着各种各样的信息安全威胁，如计算机病毒、网络黑客、恐怖分子、间谍、出卖商业机密、内部人员欺诈与恶意行为、计算机犯罪、信息处理设施滥用、自然灾害等，在全球范围内因信息安全造成的损失呈上升趋势。

1988 年 11 月，发生了一起震惊世界的计算安全事件——“莫里斯蠕虫”事件，造成 6 200 多个用户系统瘫痪，直接经济损失 9 200多万美元。

自 1987 年以来，全世界已发现超过 50 000 多种计算机病毒，2000 年 5 月爆发的“爱虫”病毒就给全球用户造成了 100 多亿美元的损失；美国每年因信息与网络安全问题所造成的经济损失高达 75 亿美元。

2001 年，恐怖分子利用 internet 策划、实施了举世震惊的 9.11 事件，造成高达 400 多米的美国世界贸易大厦化为一堆废墟，有数千人遇难。

英国巴林银行职员里森在新加坡从事金融衍生交易，因其交易权力过于集中(同时一人身兼首席交易员和清算主管两职)及巴林银行对其监管不力，造成交易亏空长期隐瞒不报，最终导致具有 233 年历史、在全球范围内掌管 270 多亿英镑的英国巴林银行宣告破

产，最后被荷兰某集团以 1 英镑象征性地收购。

2001 年 2 月 21 日，美国联邦调查局 FBI 逮捕了其资深雇员(资深程序员)汉森，美国联邦调查局在法庭上出示了长达 108 页对其进行间谍活动的指控书，指出在过去的 15 年里汉森窃取了美国联邦调查局大量机密文件，通过磁盘将其卖给俄罗斯。

美国联邦调查局统计的结果表明，65％的攻击来自网络系统内部。黑客的侵扰也是个极大的破坏信息安全的重要因素，目前，因特网上已有 3 万多个黑客网站，而且技术不断创新，基本的攻击手法已多达 800 多种。即使是防卫森严的美国国防信息系统 2000 年也受到 25 万次的黑客攻击，且成功进入率高达 63％。

最近几年我国经济一直保持高速发展，通信技术与网络技术迅猛发展，人员频繁流动，同样也面临着信息安全问题，信息安全事件也屡见不鲜。

2001 年由公安部公共信息网络安全监察局组织举办的我国首次计算机病毒疫情调查，调查结果显示：中国有高达 73％的计算机曾遭受病毒感染，而且多次感染现象非常严重。

截至 2001 年底，我国已有网民 3 370 多万人，上网计算机 1 254万台，其中政府域名超过 5000 个，信息安全问题也已大量出现。国防科技大学计算机学院所作的研究课题表明，目前我国 95％的与因特网相连的网络管理中心都遭到过境内外黑客的攻击或侵入，其中银行、金融和证券机构是黑客攻击的重点。

1987 年 7 月，发现第一起金融计算机犯罪案件，中国银行深圳某支行被诈骗 5 万元。

1996 年 11 月 4 日，人民银行全国电子联行系统因局部通信故障，导致 28 亿元资金滞留 2.5 天，海南等地因此出现头寸紧张，支付困难的局面。

2001 年，北京、广东等地发生多起股票盗买盗卖事件，涉及金额 100 多万元。

2001 年 12 月 27 日，烟台市人民检察院依法对涉嫌伪造有价

票证的犯罪嫌疑人乔××批准逮捕。乔××利用到某电信公司维护通信设施之机，通过修改数据库伪造 200 电话卡 10 000 张，给该电信公司造成 20 余万元的经济损失。

2001 年 2 月 9 日上午 8 时左右，中美之间的一条海底光缆在日本横滨维护区(位于我国上海崇明海底光缆站以东 375 千米的公海中)发生阻断，造成中国电信及其他电信运营商北美方向部分电路中断。中美海底光缆是承担中美间因特网数据交换的重要载体，其中中国电信就有 930 兆的因特网互联电路，中国联通、中国网通也有部分因特网互联电路在这条海底光缆上。在海底电缆发生阻断后，这些互联电路随即中断，网民访问北美地区的网站因此受到影响。

据新华社南京 2000 年 3 月 11 日晚报专电：江苏省徐州市某银行的软件维护员孙××堪称“超级黑客”，他只在银行存过 10 元钱，却凭自己的电脑技术改动存款记录，半年多来从银行取走了 33.8 万余元。徐州市云龙区法院以贪污罪判处他有期徒刑 5 年。

2001 年发生的轰动全国的湖北“4.20”体育彩票案，犯罪嫌疑人章××通过窃出彩球并将彩球在家用刀沿中线将球切开，放入螺母，贴上透明胶，然后，又回到博彩厅将球按“7171691”的顺序装入摇奖器，自己又在某彩票销售点购买了一组 5 注含“717691”号码的彩票，但在摇奖过程中有一彩球被卡住，未能成功。

河南焦作律师于×因犯泄漏国家秘密罪，2001 年 4 月 28 日被沁阳市法院一审判处有期徒刑一年。据悉，这是我国首例在职律师因泄漏国家秘密而被判刑的案件。律师于×在担任×××涉嫌贪污一案的辩护人时，在贪污犯罪嫌疑人家属的要求下违反规定，授意其同事将案卷材料复印件连同一份起诉书留给嫌疑人家属，致使嫌疑人家属进行一系列反侦查活动，导致有关证词一翻再翻，使该案两次延期审理，在当地造成恶劣影响。

现年 29 岁的袁×与妻子孔×，大学毕业后分配在西安的一家

国防单位工作，共同参与了该单位的重要国防科学研究项目。他们在工作期间，曾将属于国家机密的一些资料私自带回家中。2000年6月，受江苏省的一家研究所的高薪聘请，袁氏夫妇决定前往南京工作，离职时还将平日非法获取的原单位的秘密图样、资料也一并带走。2000年7月，公安机关接到举报，依法立案侦查，查明了袁氏夫妇的踪迹。警方在其住所查获了标明国家机密的软盘、图样、原始试验记录本和技术说明书等物证。2001年2月20日，西安市雁塔区检察院以袁×、孔×犯非法窃取国家秘密罪向雁塔区人民法院提起公诉。雁塔区法院经过不公开审理认为，袁×、孔×的行为已构成非法获取国家秘密罪，鉴于两人属偶犯、初犯，且认罪态度好，可从轻处罚。遂于4月9日公开宣判，袁×和孔×被分别判处有期徒刑1年，缓刑两年。

四川某建筑机械厂的两位掌握该厂从法国某公司引进塔机专有技术的技术人员，在未办理辞职的情况下于1993年开办了一个工程机械厂，并开始生产还处于保密阶段的减速器等产品。双方经过长达3年的官司，成都市中级人民法院4次开庭，于2000年做出一审判决，被告方侵犯商业秘密成立，赔偿四川某建筑机械厂共计人民币200万元，并停止侵犯行为。据悉，这是我国首例侵犯产品关键核心部位机密案，也是建筑业的首例侵权案，引起了业内人士的广泛关注。

以上仅是在各种公开媒体上摘录的少数有关信息安全的事件。实际上信息安全所涉及的内容与领域非常广泛。在我国与信息安全有关的国家行政主管部门就有国家安全局、国家保密局、公安部、信息产业部等，他们按照各自的行政分工负责国家的信息安全管理工作。因此关于我国信息安全事件的具体统计数据不易获得，再加上许多组织出于保护商业信誉的考虑，即使发生了安全事故也不愿意对外公开，每年我国因信息安全问题所造成的经济损失也无法做出全面的评估。但是有一点可以肯定，在威胁多样化的信息化时代，我国信息安全管理的现状不容乐观，这可以从国家宏观管理与