网络远比你想像的要脆弱　信息安全的威胁通常源于内部

ENTERPRISE INFORMATION SECURITY GUIDE

企业信息安全指南

信息安全就如人生一样，是一个过程而非终点

暨南大学出版社
Jinan University Press

陈伟强　黄求新　著

ENTERPRISE INFORMATION SECURITY GUIDE
企业信息安全指南

陈伟强　黄求新　著

暨南大学出版社

图书在版编目（CIP）数据

企业信息安全指南/陈伟强，黄求新著 .—广州：暨南大学出版社，2003.7
ISBN 7-81079-261-X

Ⅰ.企… Ⅱ.①陈…②黄… Ⅲ.企业管理—计算机应用—安全技术
Ⅳ.F270.7

中国版本图书馆 CIP 数据核字（2003）第 053119 号

出版发行：暨南大学出版社

地　址：中国广州暨南大学
电　话：编辑部（8620）85226530　85226593　85221601
　　营销部（8620）85226712　85228291　85220602（邮购）
传　真：（8620）85221583（办公室）　85223774（营销部）
邮　编：510630
网　址：http://www.jnupress.com　http://press.jnu.edu.cn

排　版：暨南大学出版社照排中心
印　刷：广东惠阳印刷厂

开　本：787mm×960mm　1/16
印　张：17.5
字　数：315 千
版　次：2003 年 7 月第 1 版
印　次：2003 年 7 月第 1 次
印　数：1—5000 册

定　价：28.00 元

序 言(一)

每个时代都有自己领先的、标志性的、为之骄傲的科技产生，它们的出现大大改变了人类的生活和行为方式，推动了整个人类社会前行的步伐。然而，科技在带给人类巨大的社会效益和经济效益的同时，也遭到了一部分人的利用甚至毁灭性的破坏。当然，这种利用和破坏可能是不经意的，但更多的是蓄意的，不管出于什么目的，由此而带来的损失都不可避免。而且，这种损失的程度与科技所能创造的效益同样巨大，甚至有过之而无不及，因此，在我看来，充分发挥现代科技的应用价值与预防现代科技可能存在的危害应同等重视。事实上，由于过度追求利润以及普遍的侥幸心理，我们在后一方面尤其做得不够。

国内许多企业在越来越依赖计算机进行工作的同时，对企业信息安全的漠视就是最好的例证。下述这些现象，相信不少的企业管理者都会有所体会：新的安全漏洞公告出来很久，却无人重视和采取应对措施；难度很高的密码由于难于记住而被员工随手抄写在鼠标垫上；不断有人在企业内部拨号上网而使内网门户大开，强大的防火墙形同虚设；离职解聘员工的系统登陆账号和密码一直没有被更换和取消；好奇的员工总是点击标题诱人的恶意邮件的附件，从而让病毒有机可乘；专业财务管理的密码和普通桌面密码混用；新的安全补丁并没有在每一个桌面上进行安装，甚至公司配备专业的信息安全管理员对这种状况也一无所知；安全产品的默认密码从未变更；安全会议开了很多次但总是效果不大……当然，还有因各种技术方面的不足而导致的安全损失。这些问题的解决并没有你想像的那么困难，有些甚至是轻而易举，而不必等到要造成了巨大的损

失后才想到亡羊补牢。此书的意义不仅在于告诉你这些，它所提供的解决方案亦是当前国际信息安全领域里最先进的和全面的。

此书的两位作者都长期在国外学习和生活，且在国际知名企业积累了数十年的企业信息安全管理和实践经验。眼界高远，融会中西，知识和技能俱丰富，理论和实践皆具备。此书的出版，是两位作者智慧和心血的结晶，相信对我国企业信息安全意识的培育和引起重视亦有着重要的引导作用。

中国信息产业部信息化推进司司长
国家信息化推进工作办公室主任
中国电子商务协会理事长
宋　玲
2003 年 5 月 8 日于北京

序 言（二）

计算机在极大提高企业工作效率的同时，也带来了极具威胁的信息安全问题。一方面，企业利用计算机进行产品设计、文件制作、工作交流、数据交换、市场推广等等，公司的运营策略、销售计划、客户资料、商业机密等大量重要数据储存在计算机里；另一方面，由于计算机网络的发展，计算机又变得非常脆弱，他人通过网络利用一个小小的病毒程序，一台配置不是很先进的计算机，就能侵入企业内部的计算机系统，使你的计算机停止工作，损害或更改计算机里面的数据，窃取你计算机内部的秘密，而电脑破坏技术的发展又使得这类入侵变得防不胜防。

因此，企业在大力提升计算机系统的性能的同时，如何保证企业计算机系统的安全日益成为一个严峻的问题，《企业信息安全指南》一书正是适应这一社会问题而作的，着重从企业管理的角度来阐述计算机存在的安全隐患及其解决之策。

作者之一黄求新先生为美籍华人，在美国学业、事业皆有所成之时，心系桑梓，先后在中国香港和大陆工作、学习多年，积极参与祖国的经济建设。黄求新先生在其繁忙的工作之余，孜孜不倦，潜心求学，获得了暨南大学法学院硕士学位，目前正在中山大学管理学院、武汉大学法学院攻读双博士学位。其好学之心，实为我辈楷模。

另一作者陈伟强先生，是澳洲 RMIT 大学计算机应用科学理学士、美国东南大学工商管理硕士、英国 Warwick 大学第四方物流博士研究生，先后出任国际知名企业 GE、甲骨文（Oracle）等公司高层管理职务，目前是香港上市公司——亚洲物流科技有限公司的行

政总裁，陈先生在企业信息安全方面积累了多年的实际操作经验，并且在这一领域取得了丰富的理论研究成果。

两位作者运用自身扎实的理论基础及丰富的实践经验，历时数月写出《企业信息安全指南》一书。系统全面地介绍了信息安全的定义、信息安全所面临的威胁以及当今世界解决信息安全的最新技术、方法和措施，并且针对不同企业、不同信息保密要求，提出了不同的信息安全建议，该书还对目前信息安全中的热点问题——计算机犯罪问题以及信息安全认证新宠——信息系统安全认证（CISSP）这一国际最新认证考试进行了介绍。该书立意前瞻，构思新颖，深入浅出，具有简洁、实用和操作性强的特点，尤其适合企业经营者、企业管理层、财务及资料管理人员、信息安全管理人员等阅读、学习。本书所选用的资料也大多来自于国外最新研究成果，实为我国的企业信息安全研究领域的最新力作。

该书的出版，有助于我国企业管理人员从策略上提高对企业信息安全的认识，为各类企业在信息安全方面提供了全面而又正确的指引，是一本不可多得的好书。本人亦非常高兴为之作序。

华南理工大学电子与信息学院副院长、教授

贺前华

2003 年 5 月 15 日

自 序

在原始社会，人类已懂得用仓库、房子来储藏私人财产，用门锁和看守人员来保护更为贵重的物品。这时候，门锁、家犬及看守人员便成了最有效的工具。

在钱币和票据发展为个人重要的财产时，银行的大保险柜、最先进的时间锁、训练有素的保安人员也随之出现，他们显然比原始的门锁、家犬及赤手空拳的看守人员更为有效。

在今天，私人和公司最需要保护的物品，不是那些看得见、摸得着的物质资产，而是计算机及其信息安全，如存折密码、客户资料、重要合同、财务报表、知识产权等。据统计，全世界上市公司的品牌价值、知识产权（信息、商业秘密）等的价值已大大超越了实物资产。而这些资产——信息资料、商业秘密……无一例外地都存放在企业的计算机系统里，计算机已成了大多数企业最重要的工具和现代企业运作的命脉。而且，这种趋势正变得越来越明显和强化。

于是，一个崭新的商业环境呈现在企业家们的面前：一方面信息成为企业的战略资源，企业越来越依赖于通信和计算机网络，通过对关键流程的信息化，在提升企业效率和客户满意度的同时，也在其计算机系统里存入了企业最核心、最重要的资产；另一方面，信息系统任何原因的中断和网络数据的丢失与破坏都会给企业造成巨大甚至致命的损失，企业安全受到空前的挑战。以下就是企业信息安全方面所面临问题的最新统计数据：

美国计算机紧急事件反应小组协调中心（CERT/CC）公布的数

字显示，该中心自从1998年成立以来，收到的计算机安全事故报告的数量一直呈上升趋势，2001年该中心接到的计算机安全事故报告的数量比2000年翻了一番多，达到创纪录的52 658起。

据统计，全世界由于信息系统的脆弱性而导致的经济损失，每年达数十亿美元，并且逐年上升。

据美国《金融时报》报道，现在平均每20秒就发生一次入侵计算机互联网的事件；互联网的防火墙，超过1/3曾被攻破。

据调查，目前国内80%的网站存在安全隐患，20%的网站有严重的安全问题。一位“黑客”甚至说如果他敲键的速度足够快的话，一天可以黑掉100个网站，寻找网站的安全漏洞简直成了体力活！

面对如此环境和挑战，信息安全迅速成为企业信息化中企业家们最为关心的问题。企业家们很容易发出这样的疑问：

本企业的商业信息系统是安全的吗？

本企业的商业信息系统究竟面临着哪些安全问题？

这些无处不在、无时不在的信息安全问题将会给本企业带来怎样的危害？

本企业如何采取有效、完善的措施来防范这些信息安全问题，以彻底解除企业的后顾之忧？

本书将就以上问题，用最通俗易懂的语言和形象贴近的图表，作出全面、系统和符合企业实际的分析和探讨。我们希望，通过本书，能引起企业决策者对企业信息安全的重视，并自觉地采取一些行之有效的防范措施，以期能为您的企业带来安全、通畅、商机和财富，则幸莫大焉！

作者：（香港）陈伟强（Ringo Chan）

（美国）黄求新（Stephen Wong）

2003年5月

特别致谢

本书在编写过程中，暨南大学法学院常务副院长周显志教授，武汉大学法学院副院长、博士生导师温世扬教授，华南理工大学电子与信息学院副院长、博士贺前华教授曾给我们大力的支持和悉心的指教；中国信息产业部信息化推进司司长、国家信息化推进工作办公室主任、中国电子商务协会理事长宋玲教授，中山大学博士生导师李江帆教授，暨南大学的吕国民教授，高雄飞教授，中国电子商务协会常务理事、副秘书长张光平博士也为本书的出版提供了许多的帮助和中肯的建议；此外，邬俊、汪文宇等为本书也做了大量的工作。可以说，没有上述人士的支持和协助，本书就不会如此顺利地出版。在此，谨向以上人士表示深切的谢意！

作为一册试图全面地、系统地介绍计算机信息安全领域所面临的问题及其应对之策的专业书籍，本书有初创之功，亦有初创之失。功不敢自居，失却难逃其咎。诚望各位读者不吝赐教，在此一并致以衷心的谢意！

（香港）陈伟强（Ringo Chan）

（美国）黄求新（Stephen Wong）

2003 年 6 月 5 日

目 录

第十三章 电子商务与电子签名

第十四章 建立安全项目

第十五章 安全评估

第十六章 信息安全管理委托服务

第十七章 事件响应、升级和恢复

第十八章 确保互联网络安全性

第十九章 法律问题概述

第二十章 计算机犯罪

第二十一章 信息系统安全认证

第二十二章 总 结

第一章　何谓信息安全

重点信息　保障资料安全就是让计算机确保你个人或公司的秘密不被泄漏或盗取，完整的资料不被篡改或遗失，让你有需要时可作存取，并为每次交易提供记录。

在我们的日常生活中，大多数人都知道使用门锁、防盗网及狼狗等工具来提高家庭或办公室的安全性，其实计算机系统也同样需要相应的防范措施来提高计算机系统的安全性。不过要将现实世界可以做得到的事情转移到计算机上，就必须先弄清技术名词的定义及业务本身的需求。如果你从来没有接触过信息安全，则你很快就会知道除了防止众所周知的“黑客”外，要令你的计算机系统达到“安全”，其实还有很多事情要做。

信息安全的种类

信息安全确实存在而且刻不容缓。那么，在解决信息安全问题之前，先让我们来弄清楚我们的计算机究竟潜藏着哪些安全问题吧。

病毒

病毒与计算机相伴而生，而互联网更是病毒滋生的温床。从早期的“小球”到引起全球恐慌的“梅丽莎”，病毒时刻是最直接的安全威胁。

内部威胁及无意破坏

事实上，大多数威胁来自内部，来自同事、被解雇的职员、受信任的顾客、咨询顾问等所有能进入系统的人。此外，一些无意的行为，如丢失口令、疏忽大意、非法操作等都可以对网络造成极大的破坏。据统计，此类问题要占网络安全问题总数的70%左右。

系统的漏洞和“后门”

操作系统和网络软件不可能是百分之百无缺陷和无漏洞的，然而，这些漏洞和缺陷恰恰是黑客进行攻击的首选目标。另外，软件的“后门”都是软件公司的设计编程人员为了自便而设置的，一般不为外人所知，但一旦“后门”洞开，其造成的后果将不堪设想。例如，微软公司的Windows产品就存在此类的严重问题。

网络上的蓄意破坏

好比说在未经他人许可的情形下窜改他人网页，作案动机多半是因为政治原因或仅仅为了炫耀自己的技术。在2002年和2003年，美国发生许多类似案件，一些著名的官方、新闻及商务网站皆遭到不明黑客的入侵破坏。2002年，我国一些站点也遭到来自国外的此类恶意攻击。

侵犯隐私或者机密资料

很多人有这样的经验，当你从事网络购物或是信息的搜寻时，对方往往会要求你的信用卡资料作为注册的必要条件之一，并添加一大段文字确保此类个人资料的安全性。事实上，黑客并不需使用多么先进的技术便可获得此类资料。通常只要用偷窥信息的封装（data packet）程序，即可得知使用者的注册名称及密码，然后间接使用这些数据输入上网，调出所谓的使用者资料（personal profile）。

拒绝服务

当组织或机构因为有意或无意的外界因素导致无法完成应有的网络服务项目（例如电子邮件系统或是联机功能），即称为“拒绝服务”（Denial of service）问题。最近，YAHOO、HOTMAIL、CNN 等站点就受到此类攻击。虽然此类破坏并未直接威胁到信息的安全，然而公司本身却往往需要耗费大量的时间和精力来弥补错误。

信息安全的四个目标

🗀 重点信息　信息安全有四个目标，就是保密性、完整性、可靠使用性及不可否定性。

信息安全有四个目标：保密性、完整性、可靠使用性及不可否定性。需要特别指出的是，前三个目标对于负责信息科技的部门来说就如吃“糖果”一样，吃太多的“糖果”会令你生病，也可能令你超重。所以太严密的计算机安全水平对业务亦有负面的影响。此书能帮助你了解到信息安全应达到何等水平才适合你的业务。

保密性、完整性及可靠使用性是不可分割的，其定义及解决办法亦类似。但这不是重点所在，最重要的是，我们采取目标为本的方法：计算机应在我们需要的时候做我们需要它做的事——因为我们才是它的主人。当然，它不应为用户以外的人做任何事。

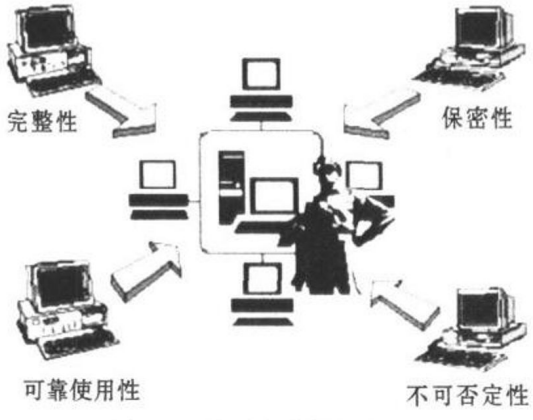

图 1-1　信息安全的四个目标