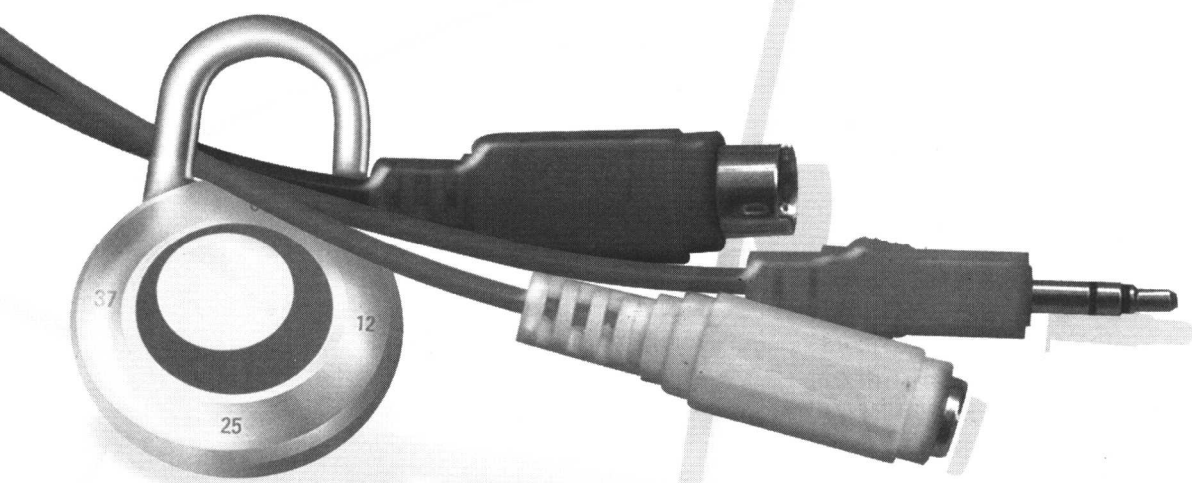
信息安全风险评估

吴亚非 李新友 禄凯 主编

清华大学出版社

信息安全风险评估

吴亚非 李新友 禄凯 主编



清华大学出版社
·北京·

内 容 简 介

信息安全风险评估理论研究日趋成熟，相关资料比较充分，但有关评估实际工作的参考资料很少。本书以信息安全风险评估实践为基础，围绕评估工作中各阶段的实际操作，分基本知识、技术与方法、产品与工具、案例四个部分，详细介绍了信息安全风险评估的基本概念、国家政策及标准发展、评估实操方法、各种实际评估表格示例、评估分析模型和计算公式、目前主要的评估工具，并从不同行业和不同评估目的出发，列举了多个评估案例，供读者参考。

本书主要面向国家和地方政府部门、大型企事业单位的信息安全管理人员，以及信息安全专业人员，可作为培训教材和参考书使用。本书对进行信息安全风险评估、风险管理、ISMS(ISO/IEC27001)认证等具有较高的实用参考价值。

图书在版编目(CIP)数据

信息安全风险评估/吴亚非，李新友，禄凯主编. —北京：清华大学出版社，2007.4
ISBN 978-7-302-14610-0

Ⅰ. 信…　Ⅱ. ①吴… ②李… ③禄…　Ⅲ. 信息系统—安全技术—风险分析
Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2007)第 014512 号

责任编辑：冯志强　刘　霞
责任校对：张　剑
责任印制：李红英
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
c-service@tup.tsinghua.edu.cn
社 总 机：010-62770175　　**邮购热线**：010-62786544
投稿咨询：010-62772015　　**客户服务**：010-62776969
印 刷 者：北京鑫丰华彩印有限公司
装 订 者：三河市李旗庄少明装订厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：18.75　**字　数**：418 千字
版　　次：2007 年 4 月第 1 版　　**印　次**：2007 年 4 月第1 次印刷
印　　数：1～4000
定　　价：35.00 元

封面设计：子时文化 (010)86390064

前言 FOREWORD

2005年12月16日国家网络与信息安全协调小组讨论通过了《关于开展信息安全风险评估工作的意见》，2006年1月6日国务院信息化工作办公室将《意见》印发中央各部委和全国各省市。《意见》是国家出台的第一份关于信息安全风险评估工作的纲领文件，标志着我国信息安全领域一项基础性、全局性的新工作正式启动。

《关于开展信息安全风险评估工作的意见》要求三年内在国家基础信息网络和重要信息系统中普遍推行信息安全风险评估工作。各行业主管部门应重视信息安全风险评估的核心技术、方法和工具的研究与攻关，积极开展信息安全风险评估的培训与交流。

为了落实和推进国务院信息办的工作要求，更好地开展培训工作，国家信息中心信息安全研究与服务中心组织了《信息安全风险评估》培训教材的编写工作。该培训教材从国家政策、技术标准、技术方法、产品工具以及实施案例几个方面，详细描述信息安全风险评估工作的主要内容。本书是在这个培训教材的基础上整理而成的。由于时间有限，加之该领域正处于研究和发展阶段，书中不足之处在所难免，敬请读者提出宝贵意见。

特别感谢中国科学院信息安全国家重点实验室赵战生教授、国家信息中心首席工程师宁家骏同志、解放军信息技术安全研究中心李京春总工和熊华博士，他们对本书的编写和修改提出了很好的意见和建议。

本书主编单位：国家信息中心；参编单位：联想网御科技有限公司、北京启明星辰信息技术有限公司、北京天融信网络安全技术有限公司、中联绿盟信息技术有限公司、Internet Security System(中国)。参加编写者有：白雷、白秋霞、崔宗军、丁一、焦大明、李明、李新友、禄凯、马岚、吴亚非、曾志强。

编　者

2006年12月

目录 CONTENTS

第一部分 基本知识

第二部分 技术与方法

第四部分 案例

第一部分　基本知识

第1章 引 论

1.1 信息与信息安全

随着以计算机和网络为代表的信息技术的迅猛发展，现代政府部门、金融机构、企事业单位和商业组织对信息系统的依赖日益加深，信息技术几乎渗透到了世界各地和社会生活的方方面面。信息系统及其所承载的信息和服务的安全性非常重要。信息和服务在保密性、完整性、可用性、可追溯性等方面出现缺陷，都将给组织机构带来负面影响。如今，遍布全球的互联网使得组织机构不仅在内部依赖信息系统，还不可避免地与外部的信息系统建立了错综复杂的联系，因此对信息加以保护的需求就尤其突出。

信息安全关注信息系统在安全方面存在的问题和面临的威胁，因此必须了解什么是信息，什么是信息安全。

1.1.1 信息

信息安全管理指南(GMITS，即ISO/IEC TR 13335)对信息(Information)的解释是：信息是通过在数据上施加某些约定而赋予这些数据的特殊含义。从广义上讲，信息是指事物运动的状态和方式，它是一种客观存在。信息是事物的一种属性，在引入必要的约束条件后可以形成特定的概念体系。通常情况下，我们可以把信息理解为消息、信号、数据、情报和知识。

信息本身是无形的，借助于信息媒体以多种形式存在或传播。它可以存储在计算机、磁带、纸张等介质中，也可以记忆在人的大脑里，还可以通过网络、打印机、传真机等方式进行传播。

对现代企业来说，信息也是一种资产，包括计算机和网络中的数据，还包括专利、标准、商业机密、文件、图纸、管理规章、关键人员等，就像其他重要的商业资产那样，信息资产具有重要的价值，因而需要进行妥善保护。

1.1.2 信息安全

信息安全(Information Security，InfoSec)自古以来就是人们关注的问题。但在不同的发展时期，信息安全的侧重点和控制方式有所不同。在通信技术还不发达的时候，面对信息安全问题，人们强调的主要是其保密性。随着电报、电话等现代通信技术的应用，防止信息在传输和存储过程中完整性受损就成了较为突出的话题。在计算机技术，尤其是网络技术飞速发展的今天，信息的可用性与其他特性都受到人们的关注。信息安全是一个广泛而抽象的概念，不同领域不同方面对其概念的阐述都会有所不同。建立在网络

基础之上的现代信息系统，其安全定义较为明确，那就是：保护信息系统的硬件、软件及相关数据，使之不因为偶然或者恶意侵犯而遭受破坏、更改及泄露，保证信息系统能够连续、可靠、正常地运行。在商业和经济领域，信息安全主要强调的是消减并控制风险，保持业务操作的连续性，并将风险造成的损失和影响降低到最低程度。

信息安全是防止信息受到各种威胁，以确保业务的连续，使业务风险最小化，投资回报和商业机遇最大化。信息安全是通过实施一系列的安全控制而达到的，包括策略、过程、程序、组织结构和软件硬件功能。必要时，需建立、实施、监视、评审和改进这些控制，以确保满足该组织的特定安全和业务目标的需要。这个过程应与其他业务管理过程联合进行。

信息作为一种资产，是企业或组织进行正常商务运作和管理不可或缺的资源。无论是对国家、组织还是个人，具有价值的信息资产都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。信息安全的任务，就是要采取措施（安全技术手段和相应的安全管理）让这些信息资产免遭威胁，或者将威胁带来的后果降到最低程度，或者进行风险的转嫁，以维护组织的正常运作。总的来说，凡是涉及到保密性、完整性、可用性、可追溯性、真实性和可靠性保护等方面的技术和理论，都是信息安全所要研究的范畴，也是信息安全所要实现的目标。

信息安全通常强调所谓 CIA 三元组的目标，即保密性（Confidentiality）、完整性（Integrity）和可用性（Availability）。CIA 概念的阐述源自信息技术安全评估标准（Information Technology Security Evaluation Criteria，ITSEC），它也是信息安全所要遵循的基本原则。图 1-1 所示即为 CIA 三元关系。

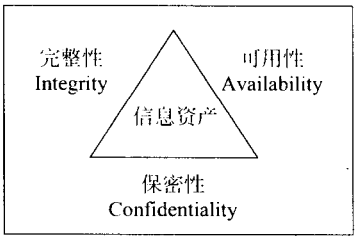


图 1-1 信息资产的安全属性

保密性（Confidentiality）——确保信息在存储、使用、传输过程中不会泄漏给非授权用户或实体。

完整性（Integrity）——确保信息在存储、使用、传输过程中不会被非授权用户篡改，同时还要防止授权用户对系统及信息进行不恰当地更改，保持信息内、外部表示的一致性。

可用性（Availability）——确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许授权用户或实体可靠而及时地访问信息及资源。

1.2 信息安全技术与信息安全管理

解决信息及信息系统的安全问题，主要取决于两个因素，技术和管理。安全技术是信息安全控制的重要手段，许多信息系统的安全性保障都要依靠技术手段来实现。但只有安全技术还不行，要让安全技术发挥应有的作用，就必须要有适当的管理程序的支持，否则，安全技术只能趋于形式或表面工作。只有将有效的安全管理从始至终贯彻落实于安全建设的各个方面，信息安全的有效性和长期性才能有所保证。信息安全是“三分靠技术、七分靠管理”，可见管理对于信息安全的重要性。

1.2.1 信息安全事件

从20世纪80年代人们开始关注信息安全到今天，信息和信息系统的威胁形式变化很大。图1-2反映了这种威胁的发展趋势。第一，从80年代以周为周期发生的安全事件，现在已经发展到以秒来计量，是原来的60万倍；第二，攻击方式在不断变化：从病毒、蠕虫、拒绝服务(DoS)攻击到现在的复合型攻击方式；第三，攻击的性质在不断变化：从个人行为，到组织行为，到目前出现国家对抗行为；第四，攻击的对象在不断变化：从针对PC、企业的服务器、业务系统直至国家的基础网络和重要信息系统。

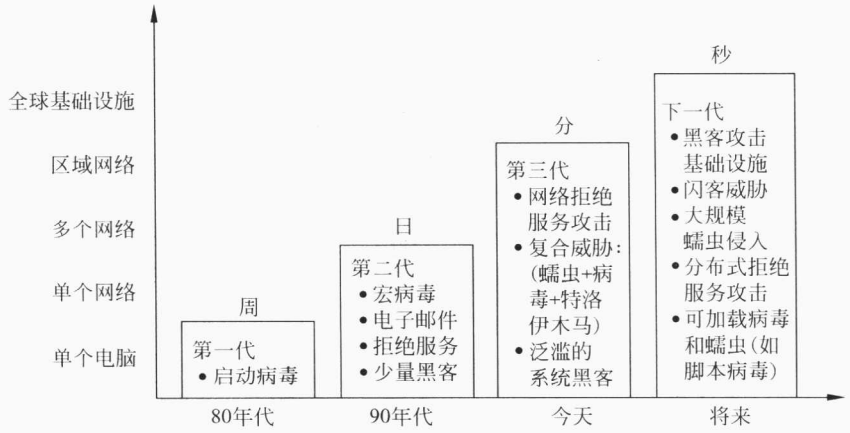


图1-2 信息安全威胁的发展趋势

例如，2005年6月17日，万事达国际信用卡公司证实，一家美国的信用卡第三方服务公司(CardSystems Solutions Inc.，Tucson，Arizona)遭到黑客攻击，该公司存储的自2004年8月1日至2005年5月27日发生交易的4000多万张信用卡账户信息可能被窃取。根据CardSystems公司公布的资料，黑客是通过一种类似于电脑病毒的脚本程序侵入CardSystems公司的电脑系统，使包括持卡人姓名、发卡机构和信用卡号在内的信用卡信息以及卡片校验码受到威胁。美国联邦调查局介入了事件调查，目前已有6.8万个账户信息可能被用于欺诈，且多数为欺诈交易。这些卡号大多涉及美国的发卡银行，交易地点波及美国、英国、加拿大、直布罗陀等国家和地区。

1.2.2 信息安全技术

信息安全技术是在攻防过程中不断发展起来的。

20世纪80年代末，由于计算机技术的高速发展引发了对计算机个体保护的强烈需求，防病毒软件得到快速发展，现在已经达到每机必备的程度。

20世纪90年代中期，网络技术的广泛应用，拉近了人们的距离，但同时也为千里之外的攻击者提供了良好的攻击运载平台。网络攻击的手段越来越多，成本越来越低，但

危害却越来越大，它可能导致：企业数据丢失、数据失密、网页篡改，进而给企业带来政治和经济上损失。网络安全需求日益强烈，由此出现了防火墙技术、入侵检测系统(IDS)、20 世纪末开始流行的抗 DDoS 系统(抗击分布式拒绝服务攻击系统)，以及目前出现的一些还不完全成熟的安全保护技术，如：IPSec、网闸等等。

1.2.3 信息安全管理

虽然信息安全技术经过了 20 多年的发展，有很多信息安全产品可以用来加强信息系统的安全，但安全事件还是经常出现。

比如，企业在进行信息系统建设时，针对薄弱环节都能进行安全保护，配置安全产品，培训安全人员等。但预期的安全目标却达不到，受到的攻击和损失依然不断增长。显然，面对层出不穷的安全漏洞和各式各样的威胁，简单的产品堆叠已经无法保证企业或组织的信息安全！

2002 年美国 FBI(联邦调查局)和 CSI 通过对 484 家公司的调查，安全威胁和安全事件研究统计表明：

- 超过 85%的安全威胁来自企业内部
- 16%的安全威胁来自内部未授权的存取
- 14%的安全威胁来自专利信息被窃取
- 12%的安全威胁来自内部人员的财务欺骗
- 只有 5%的安全威胁来自黑客的攻击

从 1995 年开始，国际上许多信息安全研究机构已经开始注意到这个问题。通过多年的研究和实践探索，信息安全界目前普遍接受了这样的结论，即只有建立信息安全管理体系，并有效地进行安全风险管理与控制，才能真正地保护组织的利益，并在信息安全事件发生的时候，将组织的损失降到最小。

信息安全管理(Information Security Management)，就是针对信息系统对象，遵循一定的原则，按照制度程序，运用恰当方法，为了完成保障信息安全的任务并实现既定目标而进行的计划、组织、指导、协调和控制等活动。对现代企业和组织来说，信息安全管理对其正常业务运行起着非常重要的作用。

信息安全管理作为一个组织的整个管理体系中一个重要环节，指导组织对其信息资产进行信息安全风险和管理。

1.3 信息安全风险评估

信息安全风险评估是信息安全管理的基础和关键环节。通过开展信息安全风险评估，对网络与信息系统的资产价值、潜在的安全威胁、薄弱环节、防护措施等进行分析，可以做到心中有数，可以发现信息系统中存在的主要安全问题，并找到解决这些问题的方法，有针对性地进行管理。

1.3.1 基本定义

信息安全风险评估是从风险管理角度，运用定性、定量的科学分析方法和手段，系统地分析信息和信息系统等资产所面临的人为的和自然的威胁，以及威胁事件一旦发生可能遭受的危害程度，有针对性地提出抵御威胁的安全等级防护对策和整改措施，从而最大限度地减少经济损失和负面影响。

1.3.2 相关概念

本节给出和信息安全风险评估有关的基本概念。

资产 Asset：对组织具有价值的信息或资源，是安全策略保护的对象。

资产价值 Asset Value：资产的重要程度或敏感程度。资产价值是资产的属性，也是进行资产识别的主要内容。

可用性 Availability：数据或资源的特性，被授权实体按要求能访问和使用数据或资源[选自国家标准 GB/T 5271.8-2001]。

业务战略 Business Strategy：组织为实现其发展目标而制定的一组规则或要求。

机密性 Confidentiality：数据所具有的特性，即表示数据所达到的未提供或未泄露给未授权的个人、过程或其他实体的程度[选自国家标准 GB/T 5271.8-2001]。

信息安全风险 Information Security Risk：人为或自然的威胁，利用信息系统及其管理体系中存在的脆弱性导致安全事件的发生及其对组织造成的影响。

信息安全风险评估 Information Security Risk Assessment：依据有关信息安全技术与管理标准，对信息系统及由其处理、传输和存储的信息的机密性、完整性和可用性等安全属性进行评价的过程。它要评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。

信息系统 Information System：由计算机及其相关的和配套的设备、设施(含网络)构成的，按照一定的应用目标和规则，对信息进行采集、加工、存储、传输、检索等处理的人机系统[选自国家标准 GB 17859-1999]。典型的信息系统由三部分组成：硬件系统(计算机硬件系统和网络硬件系统)、系统软件(计算机系统软件和网络系统软件)、应用软件(包括由其处理、存储的信息)。

检查评估 Inspection Assessment：由被评估组织的上级主管机关或业务主管机关发起的，依据国家有关法规与标准，对信息系统及其管理进行的具有强制性的检查活动。

完整性 Integrity：保证信息及信息系统不会被非授权更改或破坏的特性，包括数据完整性和系统完整性。

数据完整性 Data Integrity：数据所具有的特性，即无论数据形式作何变化，数据的准确性和一致性均保持不变[选自国家标准 GB/T 5271.8-2001]。

系统完整性 System Integrity：在防止非授权用户修改或使用资源和防止授权用户不正确地修改或使用资源的情况下，信息系统能履行其操作目的的品质[选自国家标准