企业信息安全实施指南

曾志强　编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

企业信息安全实施指南

曾志强　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书从管理和技术的角度综合介绍了企业信息安全工作的各个方面。在管理领域详细介绍了信息安全风险管理和风险评估、信息安全策略体系、信息安全事件管理、灾难恢复和业务连续性计划；在技术领域详细介绍了计算机系统安全、网络安全、数据库安全和计算机取证基础。本书不仅能够帮助读者加深对信息安全管理理论方面的理解，而且，书中列举的许多实例和解决方案可以直接用来解决日常工作中的技术实践问题，提高工作效率。

本书主要面向信息安全管理和技术人员，可以作为培训教材和参考书使用，在信息安全风险管理，信息安全策略体系设计和系统、网络、数据库安全与加固等方面具有较高的实用参考价值。

图书在版编目（CIP）数据

企业信息安全实施指南 / 曾志强编著. —北京：电子工业出版社，2008.5
ISBN 978-7-121-06410-4

I. 企… II. 曾… III. 企业管理－信息系统－安全技术－指南 IV. F270.7-62

中国版本图书馆 CIP 数据核字（2008）第 053088 号

责任编辑：万子芬（wzf@phei.com.cn） 特约编辑：徐 宏
印 刷：北京市李史山胶印厂
装 订：
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×1092 1/16 印张：18.5 字数：473.6 千字
印 次：2008 年 5 月第 1 次印刷
印 数：4 000 册 定价：38.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

随着信息技术和互联网的发展，企业正常连续运营对信息安全的依赖也越来越大。面对这样一个新兴的领域，目前绝大部分企业依然缺乏接受过系统教育和培训的信息安全专业人员以及能直接应用的技术指南。

在信息安全方面，人们往往更容易被黑客技术题材的内容所吸引，而对安全防护的内容有一定程度的忽视。实际上，对企业来说，安全防护技术远比攻击技术更为重要。这是因为：企业并不能使用攻击技术来保护自己，攻击不可能代替防守；在社会环境中使用攻击技术是违法的。而且人们往往忽略了重要的一点：攻击容易防守难，攻击者只需要找到目标的一个弱点，就可以想方设法进行攻击，而防守者则不得不考虑被保护目标的面防护甚至立体防护。

本书主要介绍了企业信息安全及其在管理、技术等领域的应用，包括企业信息安全风险分析和管理、操作系统安全、网络安全、数据库安全、安全策略体系、灾难恢复、业务连续性计划和信息安全事件管理等方面的技术和具体实施方法等。为了帮助企业相关技术人员在实际工作中能够直接参考应用一些详细操作步骤，本书从实际应用出发，对企业在 IT 环境下常见的各种操作系统（Windows 2000/XP、AIX 和 Solaris）、网络设备（思科路由器和交换机）、Web 服务器（IIS 和 Apache）、电子邮件、数据库（Oracle、Sybase 和 MySQL）等的安全和加固技术进行了详细介绍，并以 Windows 系统为例，介绍了计算机取证的一些基础知识，同时，还介绍了一些常用安全工具软件的使用方法及其在具体环境下的应用。

由于时间和精力有限，加之该领域技术更新和发展非常快，书中不足之处在所难免，敬请广大读者提出宝贵意见。

编著者

2008.5

目　录

第 1 章　为什么企业需要信息安全

"信息是商业王冠上的明珠，你的业务伙伴想知道你是否已经采取了足够的措施来保护你的信息资产。"

——Avinash Kadam

我们生活在一个信息的世界里，无数的信息环绕在我们四周，通过无线电波、电缆、光缆和其他各种相关设备不停地流进流出。大到国家大事，小到个人生活，无论是政府部门、企业，还是个人在日常工作和生活中都越来越离不开信息。尤其是在现在互联网爆炸式发展的信息社会，信息流的广度、深度和速度都是传统的信息传递手段所无法比拟的。通过网络，企业之间能够在世界各地以光速来传递各种信息，这使得现代企业能够比过去更好地适应全球化的市场和竞争。快速、准确和全面的信息能够使企业处于更好的竞争优势地位，同时也使得企业在经营过程中对现代信息技术具有越来越大的依赖性，随之而来的信息安全问题也变得越来越重要，越来越突出。

信息对那些必须使用和访问它的所有者、用户和系统等具有价值。例如，沃尔玛公司如果没有它那近 30TB（1TB=10^{12} Bytes）的数据仓库来记录和追踪成本、利润、货架周期和过去 5 年内在所有分支超市售出的所有商品记录的话，就无法有效地进行运营。航空公司如果没有使用复杂的数据库和信息系统，就无法有效地调度它那庞大的资产、人员和飞行航班。维萨和万事达组织的商业模型就是建立在卡使用数据、账户纪录、欺诈分析、消费者账单和收据基础之上，采集亿万信用卡的数据，并对卡进行收费。它们所采集起来的庞大数据库和相关信息资产本身就价值上千亿美金，比当今世界上大多数国家的年度财政预算都要大。华尔街股票交易所如果不能保证其进行交易信息的准确性，就无法正常开市，准确和可靠的信息对市场的透明度和投资者的信心来说是至关重要的。

信息具有价值，这个概念最早是由 David Nolan 博士 1982 年在他的《哈佛商业回顾》一文中提出来的。2001 年，Nolan 博士又重新表述了这个概念，并认为信息系统对企业的价值随着一系列技术演进的进程（如 1960—1980 年的大型计算机时代，1980—1995 年的微型计算机时代和现在的互联网时代）而不断增加。Nolan 博士提到微软公司利用互联网来对它的 400 000 个测试用户进行 Windows 95 软件的分发和通信。通过这些早期用户使用意见的反馈，微软公司就能在它的正式版软件投放市场前进行大量的再设计和修改。信息具有价值的概念对企业和政府来说也是非常重要的。如果信息具有很少（或者根本没有）价值的话，那么对拥有或采集它的组织来说就没有理由耗费人力、物力等资源去保护它。

1.1 信息安全定义及其历史

1.1.1 什么是信息安全

企业正常经营需要具有多种资产，如厂房、设备和人员等，对这些资产需要进行有效的保护才能保证企业不间断地正常运营。同样，信息也是一种资产，它对企业来说具有价值，因而也需要对它进行适当的保护。信息能够以各种各样的形式存在，如写或打印在纸上，存储在磁带、磁盘、硬盘和光盘上，人们之间的口头聊天，在报纸、电视和电影里等。

信息安全就是保护信息，并使之免受非授权的访问、修改、破坏和泄露等。信息安全的主要特性有以下三种。

（1）机密性：保证只有获得合法授权的用户才能访问信息，防止信息被泄露给非授权的个人、实体或过程。

（2）一致性：保护信息的准确性和完整性，防止信息被非法篡改和破坏。

（3）可用性：保证获得合法授权的用户在需要的时候能随时访问到信息。

这就是通常人们说的“CIA”法则：机密性，一致性和可用性。

信息安全可以通过实施一套合适的控制体系来实现，这套体系包括一系列的策略、行动、过程、组织结构和软件/硬件功能等。企业需要建立这套体系来确保实现特定的安全目标和任务。企业信息安全就是防止信息受到各种威胁，以确保业务连续性，使业务风险最小化，投资回报和商业机遇最大化。

1.1.2 信息安全历史

1.1.2.1 古代信息安全

信息安全并不是一个新生事物，自从人类文明发展到互相传递消息起，就产生了对保护信息安全的需要，最早的信息安全手段之一就是人们熟悉的密码学。密码学通过对信息的加密和解密，来达到保护信息机密性的目的。即便未经授权的第三方截获了被加密的信息，也无法知晓被加密前的原始信息。而加密后的信息对截获者或其他任何第三方来说只是一些无意义的数据。戴维·卡恩（David Kahn）在他那本著名的《密码破译者》一书里写到，密码学的历史最早可追溯至公元前 1900 年的古埃及人，它是从古埃及人每天交流信息使用的象形文字发展而来的。戴维·卡恩认为它是最早的有书面记载的密码学的例子之一。信息加密技术自古以来就为世界各国的军事家所重视。经典的恺撒密码（Caesar Cipher）就是古罗马征服者恺撒用来在部队中传递命令所使用，以保护军事信息不被泄露。约公元前 400 年的古希腊斯巴达人曾用一种叫做 Scytale 的木棍和羊皮纸在军事将领之间传递并加密、解密信息。在这个木棍上，斯巴达人缠上一条羊皮纸，这条羊皮纸呈螺旋形缠绕在一定直径的棍棒上。写信人在缠绕在棍棒上的羊皮纸上写下要传递的信息，然后取下羊皮纸，这样就会打乱字母的顺序，完成信息加密的工作。如果要将这条消息解密，收信人只需要将收到的羊皮纸再次缠绕在相同直径的棍棒上，这样被带过来的信件就可以恢复原来的顺序并被正常解读了。如图 1-1 所示，在 Scytale 上写上这样一则消息：“Do you want to play baseball at recess？”

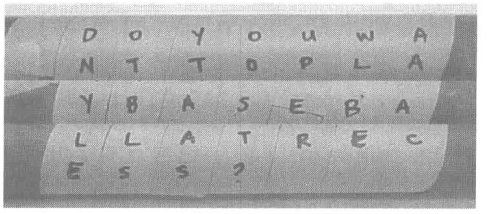

图 1-1　Scytale 示意图

我国古代的藏头诗也是一种巧妙的加密信息的方法，如施耐庵在水浒传的第六十一回“吴用智赚玉麒麟，张顺夜闹金沙渡”里，以吴用的四句藏头诗“芦花丛里一扁舟，俊杰俄从此地游。义士若能知此理，反躬逃难可无忧”传递出“卢俊义反”的信息。古代君主传达命令或征调军队需要一种信物作为凭证，这种凭证称为“兵符”。兵符由金、玉、铜、竹等材料制成，其中以铜铸的为多。已知最早的而且最有影响的是战国时期以铜铸成的虎形兵符，故称为“虎符”。一只铜老虎，一剖为两半，右半边留中央，左半边发给统兵将帅。调发军队时，君王派出的使臣拿着君王授予的半个虎符与统兵将帅持有的另外半个虎符相对，只有在两符完全吻合的情形下，统兵将帅才能按令发兵。现代汉语常用的“符合”一词，就源于此。那些闯荡江湖的民间侠客，为了在公开场合交流信息而又避免被其他人知道，也会使用他们特殊的行话。这些都属于特别的信息加密方式。

1.1.2.2　近、现代信息安全

随着社会的发展，在近、现代，信息安全这个问题变得越来越重要。信息与其他物品一样也具有价值的观念逐渐被人们接受，而且人们在生活中对信息的依赖也越来越多。近代信息安全领域的重点是信息的加密和解密。在 16 世纪著名的苏格兰玛丽女王事件中，仅仅因为玛丽女王的一封往来信件被成功解密，而导致玛丽女王本人被送上断头台。美国著名密码破译专家赫伯特·欧·亚德利在《美国黑室》一书里也详细描述了他在 20 世纪 30 年代破译日本密码电报的工作情况。现代随着计算机技术的出现、发展，尤其是互联网的飞速发展，信息安全领域发生了翻天覆地的变化。以往人们认为信息安全只与政府和军事有关，而现在信息安全却渗入到社会生活的方方面面，从企业的商业机密直到个人的信用卡账号和隐私信息的保护都让人们清醒地意识到，原来信息安全离自己很近。

在计算机网络出现和互联以前，人们只需要把资料文档等进行物理隔离，如：放入保险柜中或在企业办公地点配备 7×24h 保安人员等方式就可以有效地保护信息安全了。在互联网出现以后，企业的日常运作日益离不开 IT 系统和网络的支持，商业机密信息也逐渐转变成数字化信息并存储在相关的计算机设备里。恶意攻击者无需进入企业的办公地点就可以远程侵入企业网络，非法获取机密信息，并利用这些信息获利或给企业利益造成损害。这样，传统的信息保护方式就难以适应新形势的要求，也大大颠覆了人们心中以往的信息安全观念。下面是几个近年来的著名信息安全事故案例。

案例一：2003 年 8 月份，美国、加拿大大停电造成的灾难事件凸显了信息社会固有的脆弱性，短短几个小时内，电厂故障就引发电网崩溃，社会运转陷于瘫痪，共有 7 个主要的机场和 9 个核反应堆被迫关闭，波及美国东北部和加拿大南部的 5000 多万居民，甚至连纽约的世界银行总部的网络都被迫暂停。尽管美国政府初步排除是恐怖袭击的结果，但基地组织仍通过《世界网络日报》发表声明，称“这次袭击发电站的行动是受本·拉登指使的”。信息社会的脆弱性可见一斑。

案例二：2001 年 11 月，澳大利亚人 Vitek Boden 利用无线设备窃取了污水管理系统的控制软件，向澳大利亚河流以及昆士兰州的沿海水域中释放了 100 万升的污水。他前后共进行了 45 次入侵尝试，前 44 次入侵都未被污水管理系统检测出，这一事件暴露出澳大利亚基础设施在安全上存在一些薄弱环节。虽然 Boden 最终被判两年徒刑，但他的所作所为着实让澳大利亚政府惊出了一身冷汗。如果有人对包括铁路、汽车、公交及船运在内的全国交通体系的计算机系统进行破坏，后果不堪设想。

案例三：2006 年 6 月，中国香港金融管理局提醒香港市民提高警惕性，留意一个域名为“www.icbcasiachina.cn”的欺诈网站。该网站与中国工商银行（亚洲）有限公司［工银（亚洲）］的官方网站相似。工银（亚洲）已表明与该欺诈网站没有关系。图 1-2 是中国工商银行（亚洲）有限公司怀疑虚假网站的主页图例。

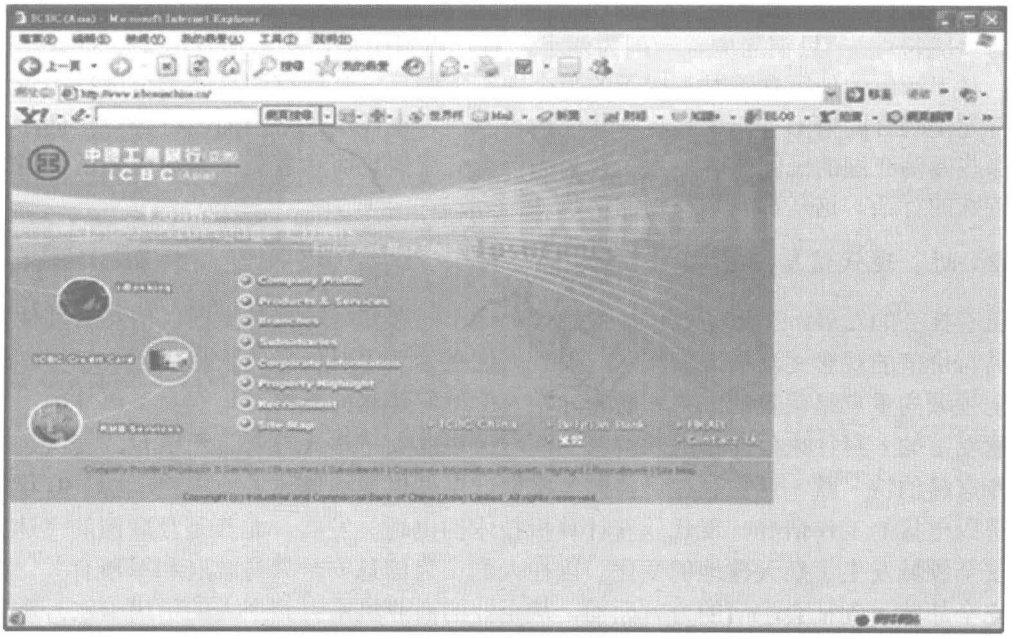

图 1-2　欺诈网站主页截图

1.2　企业为什么要保护信息安全

“21 世纪是一个被信息战和越来越多的商业间谍活动所主宰的世纪”

——美国未来学家阿尔温·托夫勒（Alvin Toffler）

1.2.1　企业对信息和信息系统的依赖

随着信息化的发展，信息和信息系统在企业里扮演着越来越重要的角色。在当今信息化社会里，信息在赛博空间（Cyberspace）里穿梭不停已成为人们日常生活中不可缺少的一部分，信息的重要性因此被人们广泛接受。信息系统通过局域网络和广域网络在企业里传递各种各样的信息，从 PC 到 PC、服务器、大型计算机等。在经营过程中，企业离不开及时的、准确的、完整的、有效的、不间断的、相关的和可靠的信息的支持。信息成为当今企业的一个重要的资源，在合适的

时间拥有正确的信息与否，往往决定着企业的赢利或亏损，成功或失败。信息共享日渐成为一种普遍的业务活动，企业的信息是一种非常有价值的、关键的资产。信息的机密性、完整性和可用性对企业的持续性经营至关重要。相应的，企业必须要确保拥有一个安全的信息系统环境。

2004 年，英国贸工部（DTI）通过对信息安全事件调查发现：一是现在有差不多 90%的企业在互联网上发送电子邮件、浏览网页和拥有网站；二是有 87%的企业把自己定义为对电子信息及其相关处理系统具有高度依赖性，而在 2002 年这个比例为 76%。可以想象，一旦这些信息系统遭遇恶意攻击或者破坏，将会给企业带来严重的甚至是毁灭性的打击。

为什么需要保护信息安全？这是因为信息及其支持过程、系统和网络等都是重要的企业资产。信息的机密性、一致性和可用性对企业的竞争力、现金流、营利、合法性和商业形象都是至关重要的。面对形形色色的威胁，信息安全能够通过保护信息来确保企业持续性运营，使其对企业造成的损害降到最低，并使企业在投资和商业机会上获得的回报最大化。在 2004 年信息安全事件调查中，英国贸工部（DTI）这样评论：“信息越来越广泛地被认为是现代企业的命脉”。在 2000 年 DTI 的调查结果中，49%的企业认为信息是关键的或敏感的，它的泄露会给企业的竞争对手带来好处。2006 年的调查结果再次确认了这一点，在调查的所有企业中，57%的企业有高度机密的信息存储在它们的计算机系统里，而在大型企业里，这个比例将高达 77%。图1-3 的数据来自于 IT 治理协会（ITGITM）的一份报告。

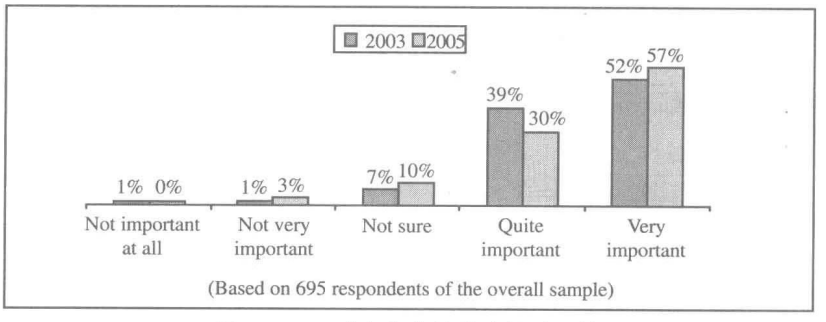

图 1-3　IT 对企业总体战略的重要性

1.2.2　企业面临的信息安全问题日趋复杂多样化

企业的信息安全可以通过多种方式被破坏，如系统故障、盗窃、不恰当地使用、非授权访问或计算机病毒等。对信息安全造成破坏的潜在影响可能会远远超过你的预期，敏感或关键业务信息丢失后不仅会直接影响竞争力和现金流，它还会破坏企业的声望，并可能带来长期的负面影响。一个企业可能要花 10 年以上的时间辛辛苦苦地建立起值得信赖的商业形象，但一个安全事件几个小时内就可以把它彻底摧毁和破坏。当企业和其他组织共享信息时，这些共享信息也需要被很好地保护起来。对很多企业来说，现在的互联网已经在很大程度上取代了传统的纸介质，成为信息交流的媒介。互联网能够使信息的发送和接收变得更快、更频繁，支持更多种类的信息传送，从简单的文本信息一直到多媒体信息。

现在已经有越来越多的企业利用互联网来进行电子商务活动和交换信息，因此，企业不得不开始注意和考虑互联网带来的一些安全问题。人们都会注意对自己的房屋、财产和人身安全进行保护，如安装防盗门、防盗网等来防止小偷和其他人员的非法闯入。同理，企业的信息也需要保护。目前，越来越多的企业遭受到信息安全事故带来的损失，这已是相当普遍

的现象，并呈现逐渐增加的趋势。在 DTI 的 2004 年信息安全事故调查问卷活动中，有超过70%的企业认为，它们曾在 2003 年经历过信息安全破坏事故。

使用信息系统能够给企业带来很多直接和间接的益处，同时也会直接和间接地带来很多与这些信息系统相关的风险。这些风险导致系统所需的保护与系统当前具有的保护之间存在着一定的差距，有很多原因导致了这些差距的产生。它们分别是：新技术的普遍应用；系统互联和网络导致距离、时间和空间的急剧缩小；各个行业技术革新的不均衡；管理和控制的权力逐渐下放；对攻击者来说，对企业进行非常规的电子攻击比进行常规的物理攻击更具吸引力；其他一些外部因素如相关法律和技术应对手段的滞后等。

信息和支持过程，系统和网络都是企业的重要业务资产。定义、实现、维持和改进信息安全对保持企业的竞争优势、现金周转、营利、守法和商业形象可能是至关重要的。企业及其信息系统和网络面临来自各个方面的安全威胁，包括计算机辅助欺诈、间谍活动、恶意破坏、毁坏行为、火灾或洪水。

造成损害的原因在于计算机病毒、黑客攻击和拒绝服务攻击等，这种现象变得越来越普遍、越来越具有攻击性和复杂化。对信息系统和服务的依赖意味着面临安全威胁的企业变得越来越脆弱。各种公用和专用网络互相连接、信息资源的共享更是增加了访问控制管理的困难度，分布式计算发展的趋势也大大削弱了过去集中化和专业化管理的效力，再加上许多信息系统在设计之初缺乏安全性方面的考虑，导致信息安全问题日趋严重。缺乏合适的管理和操作流程的支持，仅通过技术手段实现的安全是有限的，这也是近年来信息安全事故发生率呈现上升势头的重要原因之一。图1-4 是美国计算机紧急事件反应小组（CERT）协调中心的一份事故统计报告图。

1988—1989

年份	1988	1989
事故次数	6	132

1990—1999

年份	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
事故次数	252	406	773	1334	2340	2412	2573	2134	3734	9859

2000—2003

年份	2000	2001	2002	2003
事故次数	21756	52658	82094	137529

1988—2003 年事故次数：319992

图 1-4　CERT 组织安全事故统计报告图

1.3　企业信息安全问题的解决方案

问题："信息安全能做到百分之百安全吗？"
答案："不能！"

目前的信息安全解决方案能够提供的只是"信息安全风险管理"。企业要利用其拥有的资产来完成其使命。在信息时代，信息作为第一战略资源，起着至关重要的作用。因此，信息资产的安全是关系到该机构能否完成其使命的大事。资产与风险是天生的一对矛盾，资产价值越高，面临的风险就越大。信息资产有着与传统资产不同的特性，面临着新型风险。信息安全风险管理的目的就是要缓解和平衡这一对矛盾，将风险控制到可接受的程度，保护信

息及其相关资产，最终保证企业能够完成其经营使命。

在这里首先介绍几个概念：威胁、脆弱性和风险。

威胁就是那些想要进行危害的意图、一些不好的事情将要发生的迹象和可能造成危害的人或事情等。企业的信息及相关存储、处理、显示，传输信息的系统面临的威胁基本上可以分为两大类：人为的和自然的。自然威胁有雷击、火灾、洪水、台风和地震等；人为威胁有非授权系统访问、黑客程序、系统或服务偷窃、拒绝服务攻击、破坏系统和信息等。

脆弱性就是那些能够使特定的一些威胁对系统和信息造成损害的弱点。如缺少反病毒软件、缺少系统访问控制等，或其他任何能够削弱系统及系统所处理、存储、显示和传输的信息的安全性的因素。

风险就是一种特定的威胁能够利用特定的弱点来对系统和信息造成负面影响的可能性。例如，如果某个人住在一个海啸频发的海滨城市，他的系统被一次大海啸损坏的可能性就大为增加。如果没有建立一套审计日志系统，很难确定是否有人曾侵入过他的系统。

信息安全风险管理是企业信息安全保障工作中的一项基础性工作，主要表现在以下几方面。

信息安全风险管理体现在信息安全保障体系的技术、组织和管理等方面。在信息安全保障体系中，技术是工具，组织是运作，管理是指导，它们紧密配合，共同实现信息安全保障的目标。信息安全保障体系的技术、组织和管理等方面都存在着相关风险，需要采用信息安全风险管理的方法加以控制。

信息安全风险管理贯穿信息系统生命周期的全部过程。信息系统生命周期包括规划、设计、实施、运行维护和废弃五个阶段。每个阶段都存在着相关风险，同样需要采用信息安全风险管理的方法加以控制。

信息安全风险管理依据等级保护的思想和适度安全的原则，平衡成本与效益，合理部署和利用信息安全的信任体系、监控体系和应急处理等重要的基础设施，确定合适的安全措施，从而确保企业具有完成其经营使命的信息安全保障能力。

第 2 章　信息安全管理标准介绍

随着各种信息安全事件层出不穷地发生，人们越来越深刻地认识到，信息安全不仅仅是一个技术问题，同时在很大程度上也是商业、管理和法律的问题。因此，实现信息安全既需要采用技术措施，也需要借助于技术以外的其他手段，如规范安全标准和进行信息安全管理等。单纯的技术手段无法对信息资产进行全面的安全保护，仅仅依靠一些安全产品并不能完全解决信息资产的安全问题，这已经逐渐成为共识。

在全社会普遍关注信息安全的情况下，各个企业或机构都将面临遵循安全标准与相关法律、法规的要求。随着越来越多的标准、法律和法规的出台，统一安全标准的需求自然就成为一个很现实的问题。

2.1　常见国外信息安全标准

2.1.1　常见标准化组织介绍

2.1.1.1　主要国际标准化组织

国际标准化活动最早开始于电子领域，于 1906 年成立了世界上最早的国际标准化机构——国际电工委员会（International Electrotechnical Commission，IEC）。其他技术领域的工作原先由成立于 1926 年的国家标准化协会的国际联盟（International Federation of the National Standardizing Associations，ISA）承担，重点在于机械工程方面。ISA 的工作由于第二次世界大战，在 1942 年终止。1946 年，来自 25 个国家的代表在伦敦召开会议，决定成立一个新的国际组织，其目的是促进国际的合作和工业标准的统一。于是，国际标准化组织（International Organization for Standardization，ISO）于 1947 年 2 月 23 日正式成立，总部设在瑞士的日内瓦。ISO 于 1951 年发布了第一个标准——工业长度测量用标准参考温度。

IEC 也是非政府性国际组织，是联合国社会经济理事会的甲级咨询机构，正式成立于 1906 年 10 月，是世界上最早的国际性电工标准化机构，总部设在日内瓦。1947 年 ISO 成立后，IEC 曾作为电工部门并入 ISO，但在技术上、财务上仍保持其独立性。根据 1976 年 ISO 与 IEC 的新协议，两组织都是法律上独立的组织，IEC 负责有关电工、电子领域的国际标准化工作，其他领域则由 ISO 负责。IEC 的宗旨是促进电工、电子领域中标准化及有关方面问题的国际合作，增进相互了解。为实现这一目的，出版包括国际标准在内的各种出版物，并希望各个国家委员会在其本国条件许可的情况下，使用这些国际标准。IEC 的工作领域包括电力、电子、电信和原子能方面的电工技术。现已制定国际电工标准 3000 多个［注：ISO 和 IEC 一起组建了 ISO/IEC JTC1（国际标准化组织/国际电工委员会的第一联合技术委员会），这是一

个信息技术领域的国际标准化委员会。ISO/IEC JTC1 是在原 ISO/TC97（信息技术委员会）、IEC/TC47/SC47B（微处理机分委员会）和 IEC/TC83（信息技术设备）的基础上，于 1987 年合并组建而成的]。

国际电信联盟（International Telecommunications Union，ITU），是电信界最权威的标准制定机构，ITU 的历史可以追溯到 1865 年。为了顺利实现国际电报通信，1865 年 5 月 17 日，法、德、俄、意、奥等 20 个欧洲国家的代表在巴黎签订了《国际电报公约》，国际电报联盟（International Telegraph Union，ITU）也宣告成立。随着电话与无线电的应用与发展，ITU 的职权不断扩大。1906 年，德、英、法、美、日等 27 个国家的代表在柏林签订了《国际无线电报公约》。1932 年，70 多个国家的代表在西班牙马德里召开会议，将《国际电报公约》与《国际无线电报公约》合并，制定《国际电信公约》，并决定自 1934 年 1 月 1 日起正式改称为“国际电信联盟”（International Telecommunication Union，ITU）。经联合国同意，1947 年 10 月 15 日，国际电信联盟成为联合国的一个专门机构，其总部由瑞士伯尔尼迁至日内瓦。国际电信联盟包括以下两个常设机构。

（1）CCIR 是国际无线电咨询委员会的简称。成立于 1927 年，是 ITU 的常设机构之一。从 1993 年 3 月 1 日起，与国际频率登记委员会（IFRB）合并，成为现今 ITU 的无线电通信部门，简称 ITU-R。

（2）CCITT 是国际电报电话咨询委员会的简称，它是 ITU 的常设机构之一。从 1993 年 3 月 1 日起，CCITT 改组为 ITU 的电信标准化部门，简称 ITU-T。

2.1.1.2 欧洲标准化组织

欧洲标准化委员会（CEN）于 1961 年成立于法国巴黎。1971 年起，CEN 迁至布鲁塞尔，后来与 CENELEC 一起办公。在业务范围上，CENELEC 主管电工技术的全部领域，而 CEN 则管理其他领域。其成员国与 CENELEC 的相同。

欧洲电工标准化委员会（CENELEC）于 1976 年成立于比利时的布鲁塞尔，由两个早期的机构合并而成。它的宗旨是协调欧洲有关国家的标准机构所颁布的电工标准，消除贸易上的技术障碍。

欧洲电信标准协会（European Telecommunications Standard Institute，ETSI），是欧洲地区性标准化组织，创建于 1988 年。其宗旨是为贯彻欧洲邮电管理委员会（CEPT）和欧共体委员会（CEC）确定的电信政策，满足市场各方面及管制部门的标准化需求，实现开放、统一、竞争的欧洲电信市场而及时制定高质量的电信标准，以促进欧洲电信基础设施的融合。

欧洲计算机制造协会（European Computer Manufacture Association，ECMA）主要制定分布式系统安全方面的标准。

2.1.1.3 美国标准化组织

美国电气及电子工程师学会（Institute of Electrical and Electronics Engineers，IEEE）是由美国的工程技术和电子专家组建的组织，致力于电气、电子、计算机工程及与科学有关的领域的开发和研究。

美国国家标准与技术研究院（the National Institute for Standards and Technology，INST）成立于 1901 年，原名美国国家标准局（NBS），1988 年 8 月，经美国总统批准改为美国国家