科飞管理咨询公司 编著

信息安全管理丛书

信息安全风险评估

Information Security Risk Assessment

BS 7799
ISO/IEC TR 13335
GAO/AIMD-99-139
NIST SP 800-30
OCTAVE
SSE-CMM
AS/NZS 4360

中国标准出版社

信息安全管理丛书

信息安全风险评估

Information Security Risk Assessment

科飞管理咨询公司　编著

中国标准出版社

内 容 简 介

全书共分为9章，第1章～第2章主要介绍了风险评估相关的概念、风险评估在信息安全管理中的作用，以及风险评估要素之间的关系等基础知识；第3章～第9章，编者对BS7799、ISO/IEC TR 13335、GAO/AIMD-99-139、NIST SP800-30、OCTAVE、SSE-CMM、AS/NZS4360等风险评估标准/指南的发展、要素和流程以及规定的风险评估步骤做了详细的阐述。

本书的目的在于将国际国内在信息安全风险评估领域已有的良好经验以通俗易懂的方式集中介绍给国内信息安全从业人员，可为实施风险评估的组织和相关技术、管理人员提供指导和帮助。

图书在版编目(CIP)数据

信息安全风险评估/科飞管理咨询公司编著. —北京：中国标准出版社，2004
ISBN 7-5066-3656-5

Ⅰ. 信… Ⅱ. 科… Ⅲ. 信息系统-安全管理-风险分析 Ⅳ. TP309

中国版本图书馆CIP数据核字(2004)第142210号

中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码：100045
网址 www.bzcbs.com
电话：68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 787×1092 1/16 印张 14.5 字数 231千字
2005年1月第一版 2005年1月第一次印刷
*
定价 30.00 元

前　言

随着社会信息化水平的提高，信息安全问题日益突出，目前尚没有专业的信息安全事件具体损失的权威调查，但是仅从计算机病毒、黑客入侵、垃圾邮件、商业秘密失窃等事件的调查和报道中，我们不难看出信息安全建设的迫切性。我国尚处在市场经济初级阶段，工业化水平还不发达，信息安全核心技术和关键产品主要依赖于进口，这使信息化进程中的信息安全问题显得尤为重要，已成为关系国家安全的重大战略问题。当然，从全球发展的眼光来看，信息安全对任何一个国家和组织来说都是一个新课题，处在探索阶段，尚未形成相对独立完整的学科体系。坚持以安全保发展，发展中求安全，实现可持续的发展，这应该是我国当前信息安全建设的总指导思想。

大量调查表明，我国目前处在信息安全管理水平低下和意识薄弱共存的局面，导致这种现象的原因很多，例如信息化水平不高、法律法规滞后、人才紧缺、核心技术落后等，但最直接的原因是大多数的组织还不知道所面临的信息安全风险是什么。信息安全风险来自何方？有多大？需要多少投入来控制风险？所采取的信息安全控制措施是否有效？即没有风险评估的概念和方法。信息安全风险评估的目的就是识别信息安全风险并对其进行分析和

判断大小的过程，其结果可以指导信息安全方针的制定、控制目标和控制方式的选择决策以及控制效果的评估。这可以使信息安全管理有的放矢，确保控制费用与信息安全风险之间的平衡。

国际标准化组织、各国标准化组织和众多信息安全管理知名机构对信息安全风险评估进行了大量有益的探索，这些研究或以国家安全组织的有益尝试为背景，或以国际知名公司的成功经验为蓝本，博采众长，历经多年发展积累而成。本书的目的之一就是将这些已有的良好经验以通俗易懂的方式集中介绍给国内信息安全从业人员。在介绍过程中力求忠实于原文，稍有作者个人意见。其中包括风险评估的发展、概念、原理、方法和相关知识以及目前比较盛行的风险评估标准和指南，希望能够为实施风险评估的组织和相关技术、管理人员提供指导和帮助。

全书共分为9章，第1章主要介绍了风险评估的定义、风险评估在信息安全管理中的作用，以及近几年来风险评估的发展；第2章编者根据风险评估咨询的实际经验，详细介绍了风险评估相关的概念，并通过图例的方式阐明了风险评估要素之间的关系；第3章～第9章编者通过跟踪、研发目前世界范围内被普遍采用的风险评估标准/指南，对BS7799、ISO/IEC TR13335、GAO/AIMD-99-139、NIST SP 800-30、OCTAVE、SSE-CMM、AS/NZS4360等风险评估标准/指南的发展、要素和流程以及规定的风险评估步骤分别予以详细介绍。

对信息安全领域的知识与理论的探索是永无止境的，编者愿与广大读者一起，研究本书中不足的地方，共同进步。

编　　者

2004年12月13日

目　录

第1章 风险评估概述

1.1 风险评估的概念

随着人类的发展和科技的进步，信息处理的方法和技术也在不断发展，信息的传播不断加快、信息存储的媒体也越来越多，但与此同时，组织所面临的信息安全问题也不断增加，如果不采取有效的措施，信息的保密性、完整性、可用性就得不到有效的保持，而对信息的保密性、完整性、可用性造成不期望事件的主体就是信息资产所面临的威胁。威胁事件可能导致信息资产受到损害，造成资产价值降低。不同信息资产的薄弱点也不尽相同，可能是技术方面的，也可能是管理方面的。

我们可以将风险评估定义为：对风险进行识别和分析的过程，即确认安全风险及其大小的过程。安全风险的识别及判断其大小不能纯粹依照我们的主观想象来确定，它需要考虑诸如资产及其价值、资产所面临的威胁、薄弱点及组织已有的安全控制措施等多方面因素。

根据风险评估实施方的不同可将其分为自评估和他评估两类。自评估是信息系统所有者对自己系统所进行的安全风险评估，而他评估是由第二方业务关联机构或第三方中立机构提供的评估服务。由于自评估是由被评估信息系统的所有者发起的，因此涉及到一些重大问题时，其客观性、有效性和公正性也难以保证。而他评估由于其公正、公平、科学、客观，而且通常权威性也是最高的，因此应用范围最为广泛。

1.2 风险评估的必要性

随着现代政府部门、金融机构、企事业单位和商业组织对信息系统依赖程度的日益加重，信息技术几乎渗透到了世界各地和社会生活的

方方面面。信息安全和各种可能对安全造成破坏的威胁也在此消彼长的态势中得以发展和延续。在当今这个空前开放的信息化社会，与信息安全相关的风险和威胁无处不在，其中不仅仅包括网络信息系统遭受的黑客攻击，还包括通信信号中断，保险资料泄密等，下面列举了几个典型的安全事件：

事例一：

2001 年 7 月 1 日上午 8 时许开始，甘肃某通信公司因传输线路发生故障，服务处于瘫痪状态，致使部分用户信号中断近 6 小时，经过紧急抢修，当日下午 2 时许，部分用户手机陆续恢复通话。

当日上午 8 时许，在武都路营业大厅，众多用户表示，信号中断后，手机提示音却显示“欠费停机”，对此，用户觉得蹊跷，因为他们有的是 6 月中下旬缴纳的话费，有的是 6 月 30 日缴纳的话费，话费不可能很快打完。中午 12 时许，该通信公司某负责人一方面向用户发放通告，一方面解释致歉，称不久就开通并迅速开始登记停机号码。

下午 2 时许，该通信公司甘肃分公司的负责人接受记者采访时说，信号中断的主要原因是机房部分微机发生故障，致使部分用户信号中断。直到下午 4 时许，营业大厅的部分用户手机才开通，而另一部分用户仍在登记号码，等待开通。

事例二：

国内某大型银行某省分行在推动本省经济建设发展过程中，其高质量、现代化的金融服务手段吸引了众多企业和个人用户。该行逐步开展起来的多种金融业务已经服务于全省几千万用户。

但是令人意想不到的事情发生了。某日，当系统管理员执行正常的系统检测时，意外地发现系统 D 逻辑盘不见了，该盘存储了重要的 Domino 数据库文件，其中保存的是客户数据。经查三块硬盘中已经有一块硬盘停止了工作，另外还有一块硬盘存在坏道。

该行为了确保信用卡业务开展畅通无阻，采用 IBM 公司的 PC 服务器保存客户信息，结合行内专用网络和 POS 机提供前端的储蓄、结算、贷款等服务。保障信用卡业务运行的服务器是 NETFINITY 5000 系列，用双机系统形成数据备份，集成的 RAID 功能使三个 18.2G 热

插拔硬盘轻松组成磁盘冗余阵列；使用了 RAID5 以后，可以在单个磁盘损坏时，其他磁盘重新构建数据并继续工作。但是面对同时坏掉的两块硬盘，IBM 的工程师认为通过阵列已经无法成功恢复盘上数据了。在系统遭到如此严重的损坏后，只能另辟途径找回数据。

事例三：

2004 年 11 月对于在某保险公司购买车险的刘先生来说可是多事之秋。据刘先生讲述，他是 2003 年 11 月上旬在一家汽车销售公司买的车，车险还差一个月尚未到期，刘先生就开始不断接到各大车险公司的电话，询问他是否还要继续上车险，如果没有更新车险，他们愿意帮助刘先生来办理。直至刘先生续险后，这类电话仍不时响起。至今，刘先生已接到各大小保险公司的电话不下 40 个。对此，刘先生是满腹的苦恼与不解，究竟他的车险资料是怎么被泄露给这些保险公司的？

据了解，像刘先生那样曾经苦恼或是正在苦恼的车主不在少数。据另一位车主王先生讲述，他的车险快到期时也被多家保险公司“骚扰”，其中有的电话是同一家公司的不同部门。最令他感到奇怪的是自己就是在 A 公司续的保，可是仍会有 A 公司的人员打电话来询问车险事宜。发生过这类事件的车主中不乏平日对个人隐私保护得颇为谨慎的人。

事例四：

据中国日报报道，英国就业和养老金部遭遇了一场突如其来的重大事故，整个电脑网络系统几乎全线崩溃，全国 8 万公职人员被波及，这被称为英国政府历史上最大的一次电脑网络事故。

就业和养老金部是英国最大的政府部门，负责全国范围内 2400 万英国人的社会福利保障问题。该部正在执行每周例行的软件升级工作时，系统突然发生故障，全国 1000 多所办公室的 80％的台式机暂时停止工作或完全陷入瘫痪，受影响的 8 万多公职人员只能“望屏兴叹”，重操纸笔。

事例五：

英国工贸署 2004 年信息安全破坏调查报告显示英国已经彻底进

入信息时代，所有类型的公司都使用互联网。商业运作的这种改变，提高了效率并更利于顾客服务。但是提高互联的同时也存在重大的负面影响，那就是日益暴露出来的信息安全问题，信息安全问题已经成为商业生命周期中的事实。在组织努力抵抗威胁的同时，安全事故的数量持续增加。

报告中给出了英国商业遭受安全破坏的数量与 2002 年的对比数据：

- 有三分之二的英国商业组织的安全事故是由有预谋的、恶意的攻击造成的；
- 有四分之一遭受了重大的安全事故，意外的系统故障或数据破坏；
- 英国商业组织大概平均每个月都会出现一起安全破坏事件。大型商业组织每周发生一起安全破坏事件；
- 病毒感染以及员工不正确的使用系统是安全事故形成的最主要的原因；
- 不知名邮件(垃圾邮件)的数量正在快速增长，并且已经成为三分之一英国商业组织的重大问题。

通过以上的信息安全事例和数据，我们不难看出威胁是无处不在的，正是人们没有对系统所面临的威胁有一个客观的认识，没有评价威胁造成的影响，并根据评价的结果采取相应的控制措施，而导致这些安全事件的发生。这些威胁并不是突然出现的，通常是由系统一贯存在的薄弱点、人为的、或自然的破坏造成的，而且不论是信息系统还是其他支持系统(如电力、水利、交通、通信)都存在不同程度、不同类型的威胁。因此，要确保系统的安全性，确保系统正常运转，就必须首先识别、分析安全威胁，识别系统的薄弱点，评价并根据威胁发生的可能性和负面影响的程度来识别信息系统的安全风险。

信息安全风险评估是风险管理的基础，是组织确定安全要求的主要途径。只有通过风险评估识别组织所面临的安全风险，并确定风险控制的优先权，才能对其实施经济、有效的控制，从而将风险控制在组织可以接受的范围之内。没有准确及时的风险评估，将使组织无法对其信息安全的状况做出准确的判断。因此，风险评估应当成为组织建立信息安全保障体系的优先步骤。

1.3 风险评估的历史与现状

信息安全风险评估经历了很长一段的发展时期。最初的风险评估主要致力于操作系统、网络环境，也可以称其为信息基础设施的风险评估阶段，包括薄弱点评估和渗透性测试。薄弱点评估主要是利用一些工具进行安全扫描和漏洞扫描，评估网络或主机系统的安全性并且报告系统薄弱点。这些工具能够扫描网络、服务器、防火墙、路由器和应用程序，发现其中的漏洞。通常情况下，这些工具能够发现软件和硬件中已知的安全漏洞，以决定系统是否易受已知攻击的影响，并且寻找系统薄弱点。渗透性测试工具则是根据漏洞扫描工具提供的漏洞，进行模拟黑客测试，判断是否这些漏洞能够被他人利用。这种工具通常包括一些黑客工具，也可以是一些脚本文件。

随着人们对信息资产的深入理解，发现信息资产不只包括存在于计算机环境中的数据、文档，信息还在组织中的各种载体中传播，包括纸质载体、人员等，因此信息安全包括更广泛的范围。风险评估的重点也从操作系统、网络环境发展到整个管理体系。同时，信息安全管理者发现解决信息安全的问题在于预防。在此基础上，许多国家和组织都建立了针对于预防安全事件发生的风险评估指南和方法。1985 年，美国国防部正式公布了 DOD 5200.28-STD《可信计算机系统评估准则》(TCSEC)，也称桔皮书，是大家公认的第一个计算机信息系统评估标准。受 TCSEC 的影响和信息技术发展的需要，在 20 世纪 80 年代后期，几个欧洲国家和加拿大纷纷开始开发自己的评估准则。法国、德国、荷兰和英国等欧洲国家很快就开始联合行动，并于 1990 年提出欧共体的 ITSEC，真正成型的版本 1.2 版于 1991 年由欧洲标准化委员会正式公开发表。ITSEC 主要适用于军队、政府和商业部门。加拿大也于 1989 年公布《可信计算机产品评估准则》(CTCPEC)，这是专为政府需求而设计的。1992 年底，美国结合北美和欧洲有关评估准则概念公布了《美国信息技术安全联邦准则》(FC)。

由于全球信息技术的发展，需要标准化的信息安全评估结果在一定程度上可以互相认可，以减少各国在此方面的一些不必要的开支，从而推动全球信息化的发展。1993 年 6 月，由与 CTCPEC、FC、TCSEC 和 ITSEC 有关的 6 个国家中 7 个相关政府机构集中了他们的成果，并

联合行动将各自独立的准则合成一系列单一的、能被广泛接受的 IT 安全准则。其目的是解决原标准中出现的概念和技术上的差异，并把结果 CC(通用准则)作为对国际标准的贡献提交给了国际标准化组织(ISO)。国际标准化组织于 1999 年 6 月将其作为国际标准——ISO/IEC 15408 发布。

我国于 2001 年等同采用 ISO/IEC 15408 制定了相应国家标准 GB/T 18336—2001。中国国家信息安全产品测评认证中心采用该标准作为对信息安全产品测评认证的重要依据之一。

1996 年～2000 年间，国际标准化组织和国际电工委员会共同创建了《IT 安全管理指南》(GMITS:Guidelines for the Management of IT Security)系列——ISO/IEC TR 13335。由英国标准协会(BSI)制定并于 1999 年修订的《信息安全管理标准》(BS7799)受到空前重视。BS7799-1:1999 已经在 2000 年末被采纳为国际标准，以标准号 ISO/IEC17799 发布，全名为《信息安全管理实施细则》(Code of practice for information security management)。BS7799-2:1999 也于 2002 年进行了修订。在这些标准中均将风险评估作为关键步骤阐述。

1999 年，美国总审计局总结了一些主要公司的信息安全风险评估的实践，出版了相关的文档，指导本国组织进行风险评估；澳大利亚也在 1999 年专门针对风险管理制定了国家标准《风险管理指南》(AS4360)，但其只描述了过程并没有提出具体的方法；2001 年，美国国家标准与技术协会(NIST)推出的 SP800 系列的特别报告中也涉及到风险评估的内容，主要是为了组织更好地管理与 IT 相关的任务的风险，进行信息安全自我评估；2001 年，卡耐基·梅隆大学为了组织指导自身的信息安全风险评价推出了 OCTAVE 方法的 2.0 版本。

西方国家在实践中不断发现，风险评估作为保证信息安全的重要基石发挥了关键的作用。风险评估模型也从借鉴其他领域的模型发展到开发出适用于信息安全风险评估的模型。风险评估方法的定性分析和定量分析不断被学者和安全分析人员完善与扩充。最主要的是，风险评估的过程逐渐转向标准化。

第2章 信息安全风险评估原理

2.1 概述

信息安全风险评估的目的是为安全控制的选择提供决策信息，是风险管理的基础。风险管理的实际就是要以可接受的费用识别、控制、降低或消除可能影响信息系统的安全风险，风险评估的目的就是识别所存在的信息安全风险，并确定其大小的过程，为制定信息安全方针，选择适当的控制目标与控制方式提供决策依据，有的放矢，将有限的信息安全预算应用到最需要的地方，确保控制费用与安全风险之间的平衡。

风险评估是一种认识信息安全状态的方法，是在现有信息资源和安全控制条件下，对将来可能发生的信息安全事件的一种预测，这种预测是存在不确定性的。不确定产生的原因主要来自所采集信息和所选择模型两个方面。

风险评估要采集的信息一般包括信息资产(信息和信息处理设施)的价值、威胁、影响、薄弱点、已经采取的控制和事件发生的可能性等，这些信息是风险评估过程的输入，其充分性和准确性直接影响风险评估结果的可信度。在现实评估实践中，所采集信息都是有限的，其准确性也是相对的，如何克服信息和知识的不足，尽可能降低风险评估结果的不确定性具有现实的重要意义。

风险评估的模型是解决评估所采集信息和风险评估结果对应问题的，无论采用定性或者定量的方法，笼统地讲都可以把模型看成一个函数，在采集的信息相同的情况下，选择不同的模型其评估结果也可能不同。

2.2 风险评估相关定义

- **信息安全**(Information security):对信息的保密性(Confidentiality)、完整性(Integrity)和可用性(Availability)的保持。[BS 7799-2:2002]
- **保密性**(Confidentiality):确保信息仅仅为那些被授权使用的人获取。[BS ISO/IEC 17799:2000]
- **完整性**(Integrity):保护信息及其处理方法的准确和完整。[BS ISO/IEC 17799:2000]
- **可用性**(Availability):确保授权使用人在需要时可以获取信息和使用相关的资产。[BS ISO/IEC 17799:2000]
- **资产**(Asset):对组织有价值的任何事物。[ISO/IEC TR 13335-1:1996]
- **威胁**(Threat):可能对系统或组织造成损害的事件的潜在原因。[ISO/IEC TR 13335-1:1996] 这个概念明显带有 IT 背景的痕迹,笔者认为定义为"可能对资产或组织造成损害的事件的潜在原因"更适合。
- **薄弱点**(Vulnerability):指资产或资产组的能被威胁利用的薄弱点。[ISO/IEC TR 13335-1:1996]
- **风险**(Risk):某事件发生的可能性及其后果的结合。[ISO Guide 73:2002]
- **风险管理** (Risk Management):指导和控制组织相关风险的协调的活动。风险管理活动一般包括风险评估、风险处理、风险接受和风险沟通。[ISO Guide 73:2002]
- **风险接受**(Risk Acceptance):决定接受某项风险。[ISO Guide 73:2002]
- **风险分析**(Risk Analysis):系统使用相关信息,识别风险源并估计风险的过程。[ISO Guide 73:2002]
- **风险赋值**(Risk Evaluation):对照给定的风险准则和正在估计的风险,以确定风险严重程度的过程。[ISO Guide 73:2002]
- **风险评估**(Risk Assessment):风险分析和风险赋值的整个过程。[ISO Guide 73:2002]
- **风险处理**(Risk Treatment):选择并实施对策以减轻风险的处理过程。[ISO Guide 73:2002]

2.3 风险要素关系模型

2.3.1 风险要素之间的关系

通常我们把信息资产、威胁、薄弱点、控制措施统称为风险要素，这些要素之间不是互相独立的，它们存在着复杂的相互关系，图 2-1 显示了风险要素之间的主要关系，归纳起来有以下几点：

- 资产具有价值；
- 资产本身具有薄弱点；
- 威胁利用可被利用的薄弱点对资产造成影响；
- 安全控制可以降低威胁利用薄弱点产生的风险；
- 实施安全控制后仍然会有残余风险存在。

这几点类似于传染病流行的三个必要环节：传染源、易感人群和传播途径。传染源就像是威胁，某型人群缺乏对特定病毒的免疫力就像是薄弱点，隔离传染源、切断传播途径、提高人群免疫力就像是采取控制措施。

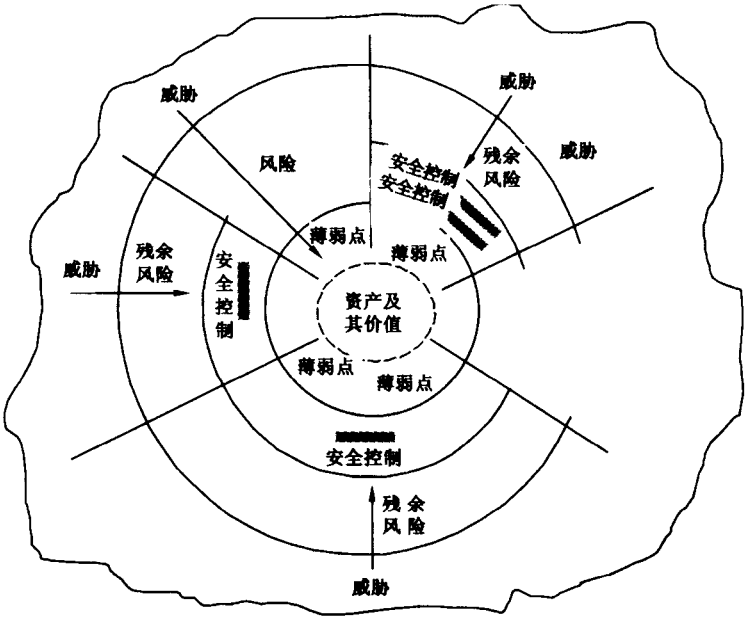

图 2-1 风险要素关系图

2.3.2 风险及其要素之间的关系

要识别风险就必须对风险要素进行识别、估价，再对这些要素的值进行函数计算得到风险值。风险和这些要素之间的关系如图 2-2 所示。

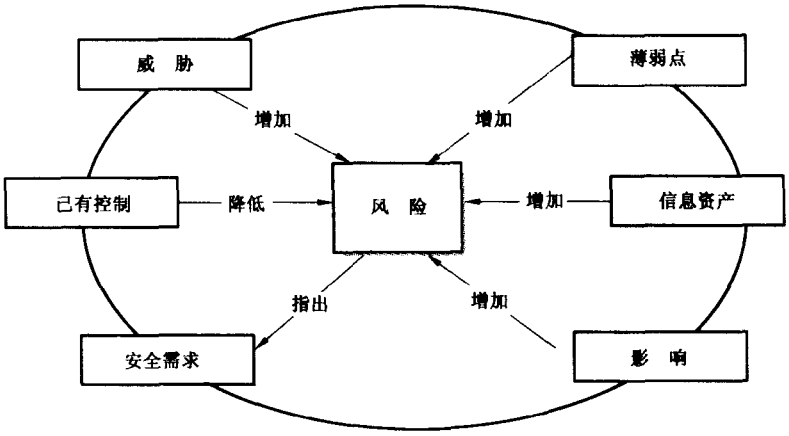

图 2-2 风险及其要素之间的关系模型

图 2-2 显示了风险要素和风险之间的关系。风险是信息资产、威胁、薄弱点、影响 4 个因素的单调递增函数，是已有控制的单调递减函数。即在其他变量保持不变的前提下：

- 资产价值越高，风险越大；
- 威胁越大，风险越大；
- 薄弱点越大，风险越大；
- 安全事故的影响越大，风险越大；
- 适当的安全控制可以降低风险；
- 安全风险指出组织的安全要求。

另外，资产、威胁、薄弱点、影响和控制等要素，不是一对一的简单对应，而是多对多的复杂映射关系。每项资产可能面临多个威胁，每个威胁可能利用多个薄弱点，特定威胁利用特定薄弱点可能产生多种影响，而针对某特定风险组织也可以选择不同的控制方式。