海军新军事变革丛书

总策划：魏　刚　　主　编：马伟明

信息系统中的风险管理（第二版）

[美] Darril Gibson　著

徐一帆　吕建伟　史跃东　译

吴晓平　主审

MANAGING
RISK IN INFORMATION
SYSTEMS, 2E

中国工信出版集团　電子工業出版社 PUBLISHING HOUSE OF ELECTRONICS INDUSTRY http://www.phei.com.cn

海军新军事变革丛书

信息系统中的风险管理（第二版）

MANAGING RISK IN INFORMATION SYSTEMS, 2E

[美] Darril Gibson 著

徐一帆 吕建伟 史跃东 译

吴晓平 主审

電子工業出版社

Publishing House of Electronics Industry

北京 · BEIJING

版权贸易合同登记号 图字：01-2016-0781

图书在版编目（CIP）数据

信息系统中的风险管理：第二版 /（美）达瑞尔·吉布森（Darril Gibson）著；徐一帆，吕建伟，史跃东译. —北京：电子工业出版社，2018.1
（海军新军事变革丛书）
书名原文：Managing Risk in Information Systems, 2e
ISBN 978-7-121-33197-8

Ⅰ. ①信… Ⅱ. ①达… ②徐… ③吕… ④史… Ⅲ. ①信息系统－风险管理 Ⅳ. ①G202

中国版本图书馆 CIP 数据核字（2017）第 303182 号

责任编辑：张 毅
印 刷：三河市鑫金马印装有限公司
装 订：三河市鑫金马印装有限公司
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：720×1000 1/16 印张：29 字数：464 千字
版 次：2018 年 1 月第 1 版
印 次：2018 年 1 月第 1 次印刷
定 价：105.00 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）88254888，88258888。
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。
本书咨询联系方式：（010）57565890，meidipub@phei.com.cn。

海军新军事变革丛书

信息系统中的风险管理（第二版）

主审　吴晓平
主译　徐一帆　吕建伟　史跃东
翻译　谢宗仁　王广强　张国华

《海军新军事变革丛书》第二批总序

当今世界，国际战略格局正在发生深刻变化。传统安全和非传统安全威胁因素相互交织，霸权主义、强权政治有新的表现，恐怖主义、极端主义、民族分裂主义此起彼伏，和平与发展的车轮在坎坷的道路上艰难前行。

发端于20世纪70年代的世界新军事变革，从酝酿、产生到发展，经历了近四十年由量变到质变的过程。海湾战争、科索沃战争、阿富汗战争及伊拉克战争这几场高技术条件下局部战争确定了世界新军事变革的发展轨迹和基本走向，展现了未来信息化战争的主体框架。这场新军事变革就是一场由信息技术推动，以创新发展信息化的武器装备体系、军队编制体制和军事理论为主要内容的世界性军事变革。

世界军事变革大势促使军队改革步伐加快。世界范围的军事变革正在加速推进，这是人类军事史上具有划时代意义的深刻变革。美国凭借其超强的经济和科技实力，加快部队结构重组和理论创新，大力研发信息化武器装备，积极构建数字化战场与数字化部队。目前正大力深化军事转型建设，通过发展航空航天作战力量等40多项措施，进一步提高军队信息化程度和一体化联合作战能力。俄军也以压缩规模、优化结构、组建航天军、争夺制天权等为重点，全面推行军事改革，着力恢复其强国强军地位。英、法、德等欧洲国家和日、印等亚洲大国，则分别推出军队现代化纲领，努力发展最先进的军事科技，谋求建立独立自主的信息化防务力量。

世界新军事变革的发展趋势是：在人才素质方面，加速由简单操作型向复合知识型转化；在军事技术方面，加速由军事工程革命向军事信

息革命转化；在武器装备方面，加速由机械化装备向信息化装备过渡；在战争形态方面，加速由机械化战争向信息化战争转变；在作战理论方面，正在酝酿着全方位突破；在军事组织体制方面，正朝着小型化、一体化、多能化的方向发展。此外，诸如战争本质、军事文化、军事法规等方面都在悄然发生变化。

胡锦涛同志指出："我们要加强对世界新军事变革的研究，把握趋势、揭示规律，采取措施、积极应对，不断加强国防和军队现代化建设，为全面建设小康社会、加快推进社会主义现代化提供可靠的安全保障。"今天的人民海军正承担着完成机械化和信息化建设的双重历史任务，时不我待，形势逼人，必须顺应潮流，乘势而上，积极推进中国特色军事变革，努力实现国防和军队现代化建设跨越式发展。

信息时代的人民海军，责无旁贷地肩负着国家利益拓展、保卫领土完整的历史重任，我们只有以大胆创新和求真务实的精神全面推进军事技术、武器装备、作战理论、体制编制、人才培养等方面的变革，才能赶上时代的步伐，逐步缩小与西方强国之间的差距，最终完成信息化军队建设的重大任务，打赢未来的信息化战争。

根据海军现代化建设的实际需求，二〇〇四年九月以来，海军装备部与海军工程大学以高度的政治责任感和思想敏锐性，组织部分学术造诣深、研究水平高的专家学者，翻译出版了《海军新军事变革丛书》。丛书着重介绍和阐释世界新军事变革的"新"和"变"。力求讲清世界新军事变革进入质变阶段后的新变化、新情况，讲清信息化战争与机械化战争、信息化军队建设与机械化军队建设在各个领域的区别和发展。其中，二〇〇四年至今陆续出版的第一批丛书，集中介绍了信息技术及其应用，出版以来深受读者好评。为更好地满足读者的需求，丛书编委会编译出版了第二批系列丛书。与第一批丛书相比，更加关注武器装备、军事思想、战争形态、军队建设编制等全局性问题，更加关注大型水面舰艇、新型潜艇、作战飞机、

远射程导弹等新一代武器装备，是第一批系列丛书的发展深化。

丛书编委会和参加编写的同志投入了很大精力，付出了辛勤劳动，取得了很好的成果。相信第二批丛书为深入学习领会军委国防和军队建设思想、了解和研究世界新军事变革提供有益的辅助材料和参考读物，在加速推进中国特色军事变革的伟大实践中发挥应有的作用。

中央军委委员
海 军 司 令 员 吴胜利

二〇〇九年七月十五日

序　言

本书的目的

本书是 Jones & Bartlett Learning 出版社信息系统安全与保障丛书中的一部。该丛书为信息技术安全、网络安全、信息保障、信息系统安全相关课程而设，是对这些关键领域的最新思考和趋势，并对这些领域秉承持续而广泛的关注。丛书标题体现了与现实应用及案例密切相关的信息安全基本准则。该丛书由多位注册信息系统安全专家（CISSP）担任作者，介绍了信息安全的全方位信息，并由信息安全领域领先的技术专家逐一审稿。本丛书不仅立足当前，而且具有前瞻性思考，引导读者应对当今及未来的网络安全挑战。

本书为信息系统中的风险管理提供了一个广泛而综合的视角，既涵盖了风险和风险管理的基本原理，又包括了更为广泛的风险管理问题细节。本书主要包括以下三个部分。

第一部分是风险管理业务的挑战，主要介绍当今管理业务的相关问题，涵盖风险、威胁及漏洞的细节，有助于读者理解组织机构中风险管理的重要性，并包含了许多管理风险的相关技术。这部分内容还详细介绍了当前在组织机构中彼此密切相关的诸多法规，并用一章的篇幅论述了风险管理计划的相关内容。

第二部分是风险缓解，重点是介绍关于风险评估的内容，主要介绍了各种不同的风险评估方法及其实施步骤，涵盖了资产识别、潜在威胁与漏洞识别的重要性。这部分内容用一章的篇幅介绍了用于风险缓解的各类控制措施，并在其他章节中介绍了如何制定组织机构的风险缓解计划，以及如何将风险评估转化为风险缓解计划。

第三部分是风险缓解计划，涵盖风险缓解计划的诸多要素，包括业务影响分析及业务持续性计划。这部分内容的最后两章具体介绍了灾难恢复及计算机事件响应小组计划的相关内容。

本书的阅读方法

本书表达风格实用通俗，通过文字描述将信息安全概念和程序的相关案例清晰地呈现给读者。文中图表既能清晰简洁地表达内容，又丰富了内容的展现形式。每章小结为读者提供了内容要点，有助于读者了解相关概念的重要性。

适用本书的读者范围

本书适用于计算机科学、信息科学专业本科生和研究生，两年制技术学院或社区大学拥有相关技术基础背景知识的学生，以及了解信息技术安全基础并希望扩展相关知识的读者。

译 者 序

随着信息系统广泛而深刻地进入和改变人们的生活，信息安全已不再仅仅是大学课堂或科幻电影所讨论和演绎的话题。在刚刚过去的不平凡的2016年，以黑客攻击为代表的信息系统安全威胁挑战国际组织、搅动社会舆论，目标甚至指向超级大国的总统大选。2016年12月美国一家安全公司Recorded Future宣称，负责测试和认证投票系统的美国选举援助委员会（EAC）遭到了黑客攻击。2016年12月16日美国联邦调查局和中央情报局根据调查报告认为，俄罗斯黑客入侵了民主党个人邮箱、曝光众多邮件，干扰了美国大选的民意走向。时代周刊甚至将2016年称为“黑客之年”。

信息系统所面临的风险和挑战业已成为任何国家、组织和个人都无法回避的重大问题。在国防领域，国防信息化建设是以信息技术为基础，对国防建设各方面进行信息化改造，实现军事指挥和控制的自动化，以提高军队战斗力。军事领域中军用信息系统作为军方搜集、分析、处理信息的平台，是现代战争指挥、通信、后勤保障等诸多决定战争胜负关键因素的依靠和保证。然而，军事组织的信息化程度与其所面临的风险成正比。在国防信息化建设过程中，以计算机网络为基础的信息系统的广泛建设和应用，使得军事信息面临着越来越严重的威胁。风险管理是信息安全的基础工作和核心任务之一。当军事训练、指挥决策、后勤保障、情报传输等基本军事活动越来越依赖于计算机网络时，军事信息系统面临的安全风险益发凸显。面对日益增长的信息系统安全需求，开展军事信息安全风险管理十分必要。如何分析和构建安全的军用信息系统，如何科学地加强风险管理至关重要。信息系统安全伴随信息系统的全寿命周期，科学有效地管理信息系统安全涉及的风险问题，具有重大的战略意义和军事效益。

本书是美国 Jones & Bartlett Learning 出版社关于信息系统安全与保障系列丛书的一部，是针对信息技术安全、网络安全、信息安全保障等背景的专著。本书从综合、系统的视角，探讨信息系统中的风险管理问题，既包含了风险和风险管理的基本原理，又深入到风险管理中各项子问题的细节，主要内容包括以下三部分。

1. 信息系统风险管理面临的挑战：涵盖风险、危害、系统漏洞的本质和细节、风险管理的技术方法、当前所涉及的法律、法规和标准、风险管理计划等内容。

2. 信息系统风险管理的风险缓解：涵盖各类风险评估方法、信息系统风险评估的完整流程、对信息系统涉及的各类资源及可能所受潜在威胁的辨识方法、信息系统风险缓解的控制类型、在组织机构中信息系统风险缓解要素的认定，以及风险评估成果向风险管理计划的转化问题。

3. 信息系统风险管理的风险缓解计划：涵盖业务影响分析、业务持续性计划等风险缓解计划中的关键要素，对信息系统灾难恢复及应急事件响应等问题亦做了翔实的探讨。

由于本书论述风格和内容组织方式与中国读者的习惯存在一定差异，下面对相关历史沿革、主要方法及相关标准体系作简要介绍，以方便读者在阅读本书之前对信息系统安全及风险管理有一个概貌性的了解。

一、信息系统风险管理的发展历史

风险管理是信息安全的基础工作和核心任务之一。20 世纪 60 年代风险管理理论应用于信息系统及信息安全领域。到目前大致经历了三个发展阶段。

1. 信息系统风险管理理论及实践的初期阶段（20 世纪 60—80 年代）

20 世纪 60 年代，随着资源共享计算机系统和早期计算机网络的出现，计算机安全问题初步显现。1967 年美国国防部委托兰德公司等多家研究机构进行了为期 3 年的第一次大规模计算机安全风险评估，出版的《计算机安全控制》奠定了国际安全风险评估的理论基础。在此基础上，美国率先

推出了首批关于信息安全风险管理及相关的安全评测标准，其中包括美国国家标准局制定的自动数据处理系统物理安全和风险管理指南及风险分析指南，还包括美国国防部国家安全局制定的 40 余项计算机系统安全评估系列标准（由于采用不同颜色的出版物封皮，俗称“彩虹系列”）。

2. 信息系统风险管理理论及实践的发展和逐步成熟阶段（20 世纪 80 年代末—90 年代末）

美国于 1989 年率先建立了计算机应急组织，1990 年建立信息安全事件应急国际论坛，1992 年国防部建立了漏洞分析与评估计划，1995 年国防部提出了“防护—监测—反应”（PDR）的信息安全动态模型，1997 年国防部发布了《信息技术安全认证和批准程序》（DITSCAP），成为美国涉密信息系统安全评估和风险管理的重要标准和依据。同期，其他国家也开始制定本国的信息安全测评标准。其中代表性的有：1993 年欧美 6 个国家启动建立共同测评标准（即后来的 CC 标准，被国际标准化组织采纳为国际标准 ISO 15408），以及英国研发的基于风险管理的 BS 7799 信息安全管理标准等。

3. 信息系统风险管理理论及实践的全球化运用阶段（20 世纪 90 年代末至今）

随着互联网、移动通信和国际跨国光缆的高速发展，信息安全成为世界各国面临的共同挑战。美国于 2002 年通过了联邦信息安全管理法案（FISMA），法案规定美国国家标准和技术委员会（NIST）负责为美国政府和商业机构提供信息安全管理相关的标准规范。该委员会发布的 NIST SP 800 系列已出版 90 余份同信息安全相关的正式文件，形成了从计划、风险管理、安全意识培训与教育及安全控制措施的一整套信息安全管理体系。2005 年，国际标准化组织（ISO）和国际电工委员会（IEC）将 2000 年发布的 BS 7799 改版为 ISO/IEC 27000 系列，形成了以信息安全管理体系为核心的、涵盖信息安全管理体系要求、风险管理、度量与测量及实施指南的信息安全管理体系，成为世界范围内被广泛接受和使用的国际认证体系。

我国也于 1999 年参照美国《可信计算机系统安全评估准则》（TCSEC），

制定和发布了《计算机信息系统安全保护等级划分标准》（GB 17859），并于 2006 年发布了《信息安全风险评估指南》，成为我国信息安全领域的里程碑。2015 年新颁布的《国家安全法》首次以法律形式提出“维护国家网络空间主权”，并在刑法修正案（九）中明确了网络服务提供者履行信息网络安全管理的义务，加大了对信息网络犯罪的刑罚力度，进一步加强了对公民个人信息的保护。

二、风险管理的主要内容和方法

风险管理的主要内容包括风险识别、风险分析、风险决策、风险控制等。

1. 风险识别

风险识别是风险管理的前提和基础，风险管理是风险识别的目的和归宿。风险识别包括确定风险来源、产生条件、确定哪些风险可能对系统构成影响。常用的风险识别方法包括头脑风暴法、情景分析法、Delphi 法、SWOT 分析、敏感性分析、问卷调查、现场勘查等。

2. 风险分析

风险分析是通过对不确定性和风险要素全面系统地分析风险发生概率及对系统的影响程度，目标是确定风险的优先级排序，弄清风险事件之间的因果关系，确定哪些事件需要制定应对措施，并有助于找到最有价值的应对措施。风险分析常用的方法包括关键路径法、PERT 法、故障树分析法、故障模式影响及危害性分析（FMECA）、事件树分析法、层次分析法（AHP）、综合分析法等。

3. 风险决策

风险决策是根据风险分析结果，制定相应对策，降低、转移、规避、分担或接受风险。这个过程包括选择合适的风险控制方式（规避、转移、降低等），确定适当的控制措施并评估剩余风险。在对策效果确认的基础上形成风险处置计划，制定风险管理策略和技术执行手段。风险决策常用的方法包括对措施的费用效益分析（CBA），以及对本领域实施措施后剩余风

险与可接受程度的度量。

4. 风险控制

风险控制是对风险的监视、管控和审查。首先是要监视和控制风险管理过程，保证过程的有效性；其次是要对成本效益进行分析与平衡，保证成本的有效性；最后是要跟踪受保护系统自身及所处环境的变化，保证结果的有效性。通过对风险的监视、管控和审查，可以及时发现各种问题，及时进行控制和纠正，保证风险管理的持续更新和改进。

虽然风险分析与管理的相关理论和技术已经十分成熟，信息系统风险分析与管理方法与其他领域中的应用十分相似，可以类比使用，但在信息系统领域的确存在一些使问题更为复杂化的特征。一般来说，认定信息安全事故并非易事，其中包含很多因素，包括不断涌现的新技术和新威胁、难以预估的蓄意行为、缺乏足够的统计数据等。如今，技术的不断发展与威胁的快速变化已成为信息系统的重要特征。因此，历史数据可能没有太多价值。另外，阻挡恶意攻击的防护措施、攻击者的动机和手段对攻击成功性影响很大，攻击往往很难预测。这些挑战与信息系统的本质不无关系，同时也反映出信息系统还远未达到人们所想象的那样成熟，信息系统风险管理从理论技术到应用实践都还有很长的路要走。

三、信息系统安全管理及风险评估标准

世界上很多国家都制定了信息安全管理及风险评估的相关标准，而本书内容主要涉及美国行业标准和相关法规。因此，下面就国内外的代表性标准作简要介绍。

1. 信息系统安全管理标准

BS 7799：BS 7799 是国际公认的信息安全管理的权威标准。它主要包括两个部分，BS 7799-1：1999《信息安全管理细则》和 BS 7799-2：2002《信息安全管理体系规范》。BS 7799-1（即 ISO/IEC 1799：2000）主要为组织机构建立并实施信息安全管理体系提供指导性准则和建议，涵盖管理要项、管理目标、控制措施及控制要点。BS 7799-2 详细说明了建立、实施

和维护信息安全管理体系的要求，并提供了建立信息安全管理体系的具体实施步骤。

ISO/IEC 13335：ISO/IEC 13335《信息技术/信息技术安全管理指南》是一个关于信息技术安全管理的指南，该标准的主要目的是提供有效实施信息技术安全管理的建议和指南，涵盖信息技术安全概念与模型、管理与计划、管理技术、防护措施的选择、网络安全管理指南等。该标准提出了以风险为核心的安全模型，阐述了信息安全评估的思路，对信息安全评估工作具有指导意义。

ISO/IEC 27001：2005：ISO/IEC 27001：2005《信息技术/安全技术/信息安全管理体系要求》是有关信息安全管理的国际标准，源于 BS 7799 标准。该标准可用于组织机构的信息安全管理体系的建立和实施，保障组织机构的信息安全，采用 PDCA（Plan-Do-Check-Action）过程方法，基于风险评估的风险管理理念，全面系统地持续改进组织机构的安全管理。

CC 标准：CC（Common Criteria）标准是目前国际上最为通行的信息技术产品与系统安全性评估准则，也是信息技术安全性评估结果国际互认的基础。CC 标准是多项标准的综合，与 ISO/IEC 15408 信息技术安全性评估准则、GB/T 18336 信息技术安全技术 / 信息技术安全评估准则符合同一标准。CC 标准定义了一套能满足各种需求的信息技术安全准则，将评估过程分为功能和保障两个部分。一方面可以支持产品中安全特征的技术性要求评估，另一方面描述了用户对安全性的技术需求。不过，CC 标准没有包括物理安全、行政管理措施、密码机制等方面的评估，且未能体现动态的安全要求。因此，CC 标准主要还是一套技术性标准。

GB/T 19715、GB/T 19716-2005：这两项标准均为信息安全管理领域的中国国家标准。GB/T 19715《信息技术/信息技术安全管理指南》与 ISO/IEC 13335 相似，亦涵盖信息技术安全概念与模型、管理与计划、管理技术、防护措施的选择、网络安全管理指南等，提供了关于信息技术安全管理的一般性指南。GB/T 19716-2005《信息技术/信息安全管理实用规则》以 ISO/IEC 1799：2000（即前面介绍的 BS 7799-1）为基础，对十大管理

要项的符合性进行了相应修改。

2. 信息安全风险评估标准

除了上述介绍的信息系统安全管理标准之外，国内外信息安全风险评估标准主要有国际的 OCTAVE、SSE-CMM、GAO/AIMD-99-139，以及国内的 GB/T 20984-2007。

OCTAVE：OCTAVE（可操作的关键威胁、资产及漏洞评估）是美国卡耐基梅隆大学软件工程研究所下属 CERT 协调中心开发的一种信息安全风险自评估方法，提供了一种信息安全风险评估规范，是从组织的角度开发的一种信息安全保护方法。OCTAVE 强调自主评估和全员参与原则，使组织机构能够厘清复杂的组织问题和技术问题。

SSE-CMM：SSE-CMM 是系统安全工程能力成熟度模型的缩写，是 CMM（能力成熟度模型）在系统安全工程领域的应用，适用于所有从事某种形式安全工程的组织，是组织和实施安全工程的通用方法。SSE-CMM 将信息系统安全工程划分为风险评估、工程实施和可信度评估 3 个相互联系的部分及 11 项关键过程，建立了横轴为 11 项系统安全工程的过程域、纵轴为 5 个能力成熟度等级的二维架构。

GAO/AIMD-99-139：GAO/AIMD-99-139《信息安全风险评估指南——向先进公司学习》是由美国审计总署（GAO）发布的对 GAO/AIMD-98-68《信息安全管理指南——向先进公司学习》的支持性文件。GAO/AIMD-99-139 有针对性地对风险评估过程进行了分析和阐述，介绍了代表性组织机构的风险评估案例，为开展类似企业风险评估工作过程提供了参考标准。

GB/T 20984-2007：GB/T 20984-2007《信息安全技术/信息安全风险评估规范》是中国在信息安全风险评估领域颁布的国家标准，涵盖风险评估框架与流程、风险评估的实施、信息系统全寿命周期各阶段的风险评估要求、风险评估的工作方式及计算方法和评估工具等内容。

四、本书的特色和使用

本书是信息系统、风险管理、信息安全等多学科领域的交叉融合之作，