HARVARD BUSINESS SCHOOL PRESS
哈佛经管图书简体中文版
全球独家授权

IT风险

TURNING BUSINESS THREATS INTO COMPETITIVE ADVANTAGE

〔美〕乔治·韦斯特曼　理查德·亨特　著
沈峰　译

不论你是企业高管、IT高管还是一般职员，你都应该读这本书，因它提供的工具、分析框架和建议能够帮助你提高IT风险管理能力，随时住机遇，迎接挑战。

商務印書館
THE COMMERCIAL PRESS

IT 风险

〔美〕乔治·韦斯特曼　理查德·亨特　著
沈峰　译

商務印書館
2011年·北京

图书在版编目(CIP)数据

IT 风险/(美)韦斯特曼,亨特著;沈峰译. —北京:商务印书馆,2011
(哈佛经管图书)
ISBN 978-7-100-07368-4

Ⅰ.①I… Ⅱ.①韦… ②亨… ③沈… Ⅲ.①信息技术—高技术产业—风险管理 Ⅳ.①F49

中国版本图书馆 CIP 数据核字(2010)第 184189 号

IT 风 险
〔美〕乔治·韦斯特曼 理查德·亨特 著
沈 峰 译

商 务 印 书 馆 出 版
(北京王府井大街36号 邮政编码 100710)
商 务 印 书 馆 发 行
北京瑞古冠中印刷厂印刷
ISBN 978-7-100-07368-4

2011 年 9 月第 1 版 开本 700×1000 1/16
2011 年 9 月北京第 1 次印刷 印张 11½
定价:27.00 元

商务印书馆—哈佛商学院出版公司经管图书

翻译出版咨询委员会

（以姓氏笔画为序）

致中国读者

哈佛商学院经管图书简体中文版的出版使我十分高兴。2003年冬天，中国出版界朋友的到访，给我留下十分深刻的印象。当时，我们谈了许多，我向他们全面介绍了哈佛商学院和哈佛商学院出版公司，也安排他们去了我们的课堂。从与他们的交谈中，我了解到中国出版集团旗下的商务印书馆，是一个历史悠久、使命感很强的出版机构。后来，我从我的母亲那里了解到更多的情况。她告诉我，商务印书馆很有名，她在中学、大学里念过的书，大多都是由商务印书馆出版的。联想到与中国出版界朋友们的交流，我对商务印书馆产生了由衷的敬意，并为后来我们达成合作协议、成为战略合作伙伴而深感自豪。

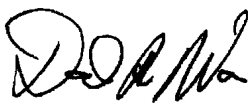
哈佛商学院是一所具有高度使命感的商学院，以培养杰出商界领袖为宗旨。作为哈佛商学院的四大部门之一，哈佛商学院出版公司延续着哈佛商学院的使命，致力于改善管理实践。迄今，我们已出版了大量具有突破性管理理念的图书，我们的许多作者都是世界著名的职业经理人和学者，这些图书在美国乃至全球都已产生了重大影响。我相信这些优秀的管理图书，通过商务印书馆的翻译出版，也会服务于中国的职业经理人和中国的管理实践。

20多年前，我结束了学生生涯，离开哈佛商学院的校园走向社会。哈佛商学院的出版物给了我很多知识和力量，对我的职业生涯产生过许多重要影响。我希望中国的读者也喜欢这些图书，并将从中获取的知识运用于自己的职业发展和管理实践。过去哈佛商学院的出版物曾给了我许多帮助，今天，作为哈佛商学院出版公司的首席执行官，我有一种更强烈的使命感，即出版更多更好的读物，以服务于包括中国读者在内的职业经理人。

在这么短的时间内，翻译出版这一系列图书，不是一件容易的事情。我对所有

参与这项翻译出版工作的商务印书馆的工作人员，以及我们的译者，表示诚挚的谢意。没有他们的努力，这一切都是不可能的。

哈佛商学院出版公司总裁兼首席执行官



万季美

序

漫议信息技术与系统风险的内在联系

我愿意向信息系统和信息管理领域的同行，以及关心信息化和信息社会的广大读者推荐乔治·韦斯特曼和理查德·亨特的这本著作，最主要的原因是该书的议题：信息技术与系统风险的内在联系。在目前已有的关于信息安全的著作中，从高层管理者的角度，对于这个议题进行深入讨论的，还没有见到。我认为，这样的研究对于我们从根本上认识信息系统的风险，从根本上提高信息管理的水平、保障信息系统的安全是很有必要的。

对于现代信息技术和复杂系统的风险之间的内在联系，或者本质联系的认识，人们是经历了一个比较曲折的过程的。几十年前，以计算机和现代通信技术为主要代表的现代信息技术开始显露出其巨大的潜力的时候，人们普遍地沉醉于它们带来的、几乎是无穷的信息处理能力之中。神话中的千里眼、顺风耳，在这一代人的时间内，迅速变成了日常生活中的现实。这样的变化在人类历史上，是空前的、十分罕见的巨大飞跃。人们在这种成就面前欣喜若狂是非常自然的、毫不奇怪的。在那段时期，几乎没有人考虑这样一个问题："大自然（或者命运，或者上帝）给了我们如此慷慨的礼物，难道就不需要有任何回报或代价吗？"事实上，在短时间内这种代价就开始显示出来了。这就是复杂系统的脆弱性，特别是大型的、复杂的信息系统的脆弱性。近年来，这一点已经开始得到了越来越多的关注和研究。从全球气候和生态危机、恐怖袭击、核泄漏和核安全，一直到北美大范围停电，大量事实已经表明，对于大系统的复杂性、脆弱性的认识和对策，是21世纪人类面临的诸多挑战背后的一个基础性的难题。而基于现代信息技术的大型信息系统的脆弱性则是其最直接、最现实的表现之一。显然，对于高级管理人员来说，这已经不是理论问题，而是非常现实的、紧迫的现实问题了。

回顾人类历史，技术进步在带来巨大效益的同时，也带来意想不到的新问题，几乎已经被证明是一条客观规律了。人们学会用火，大大提高了生活质量，也带来了火灾的隐患；抗生素的发明，提高了人们抵御疾病的能力，同时也带来了由于滥用抗生素引起的一系列问题。在这方面，最突出的例子莫过于工业化进程中的化石能源的利用了。

能源利用技术在工业革命中决定性作用是众所周知的。在一定意义上讲，工业革命给人类带来的巨大进步在很大程度上应当归功于它。然而，正是以煤和石油为主的化石能源的广泛使用，导致了环境和能源危机，从早期的伦敦酸雾到今天的全球气候变暖，人们必须面对它带来的负面效应，不得不花费巨大的人力、物力去处理其各种后果。对于大自然的这种“回报”或“代价”，人类在开始的时候也是没有认识到的，只是到了其严重后果显示出来的时候，才引起关注。（例如，著名的罗马俱乐部报告《增长的极限》）请看，这种情况和今天的现代信息技术的作用是多么的相似啊！所幸的是，人类已经从历史中得到了教益，我们不用等二三百年才认识到技术进步带来的负面效应，而是只用了不到五十年。

目前，从政府到企业对于信息和信息系统的安全正在给予越来越多的关注和投入，关于信息安全的书籍已经不少，大学里也已经在开设信息安全专业。这一切都表明，我们上面所说的理念，已经开始为各界接受。这是值得我们感到欣慰的。然而，还必须看到，目前的关注、投入以及出版的书籍，大多数还是在技术层面进行讨论，而没有从根本的理念上、从社会进步的全局上去认识和对待这件事情。正是在这个意义上，本书提供了有益的启示。作者从企业的高层管理者的角度，深入分析了现代信息技术所支持的信息系统的必然的、内在的风险，并由此提出了积极的应对策略和方法，给管理者提供了根本性的，又是切实有效的解决方案。

该书的另一个值得称道之处是，从积极的方面强调了“风险就是机遇”的重要理念。这是信息时代思维不同于工业时代思维的重要方面。工业时代的管理思想强调确定性、规范化，而把不确定性和风险简单地看成有害的、破坏性的因素，尽一切力量努力排除它们。这种思维方式的局限性在今天已经越来越明显地暴露出来，越来越不能适应社会和经济环境对于管理者的要求。信息时代的思维方式在继承了工业时代的标准化、规范化的积极成果的同时，用辩证的观点，正确地、全面地看待不确定性和风险，一方面承认不确定性是永恒的客观存在，强调正确应对而

不是试图完全消除不确定性，另一方面从积极的角度去看待不确定性和风险，认为“风险就是机遇”。事实证明，风险在创新人才看来，正是发挥创造性、开拓全新局面的难得机遇。这一理念已经在近年来得到了许多成功案例的支持。这一点在该书中得到了充分的展开，并结合现代信息技术和信息系统的实际，给出了切实可行的、现实的策略和方法。这对于今天的管理者来说是非常有益的、非常重要的。

需要说明的一点是，关于这个议题的研究应当包括企业层面和社会层面两个层次。本书作为面向管理者的读物，主要是从企业层面进行讨论，这是很自然的。目前从社会层面进行这个议题的讨论的书籍和文章还不多见。我们希望能够在不久的将来，能够见到有这方面的成果问世。

感谢译者沈峰博士和商务印书馆的辛勤劳动，使得这本书得以在比较短的时间内问世。在目前翻译工作不被认为是科学研究成果的情况下，及时地引进国外的、高水平的好书，是需要勇气和奉献精神的。因此，这是值得称道和鼓励的。

中国人民大学　信息学院　教授
中国信息经济学会　名誉理事长

陈　禹

于加拿大 多伦多

序言与致谢

要 撰写一本关于IT风险的书就如同记录描绘人生——课题如此之浩瀚，内容如此之丰富，真不知从何着手，要将什么内容写进来？如何表述？我们决定将本书的关注点聚焦在关键却被人们忽视的问题上：企业价值与IT风险管理的联系纽带。

任何企业都时刻面临各类风险。自企业开张营业，风险就降临了，直至企业歇业关门。这其中包含IT风险，其危害的可能性不断增长直至企业管理者无法再忽视它的存在。与其他任何风险一样，IT风险无法被消除，只能被管理。管理IT风险就是在风险与回报之间，在企业能够承受的风险与宁愿避免的风险之间做权衡取舍。但是，直到如今，企业的经理们还是缺少在这种意义上管理IT风险的工具。通过本书，我们将弥补这个空白。

本书将同时从IT和经营业务两个方面考虑，帮助企业经理们在面对IT风险的问题时能镇静自若的决策，确保IT风险能得到应有的管理。我们解决了以下问题：企业高管层如何认识组织中的IT风险？他们如何与IT主管一道将企业的风险轮廓勾画出来？IT主管和业务主管如何建立起管理IT风险的能力？在处理面临的风险时，他们如何一起做出合乎实情的权衡取舍？

关于本项研究

本书是基于麻省理工学院斯隆管理学院（MIT Sloan School of Management，MIT CISR）信息系统研究中心与高德纳高管研究项目（Gartner Executive Programs）大量研究的成果。本项研究调研分析了许多有效的和无效的管理IT风险的方法。通过用真实世界的案例阐释，本书提供了一个实用的方法，用来理解和

管理包含于企业 IT 资产、流程和人员之中的企业风险。

本书的基础和观点来自于我们主持的以下一些独立的研究成果：

- 由乔治·韦斯特曼(George Westerman)开展的探索性研究。研究在 11 家企业对 49 名 CIO 和他们的同行做了访谈，考察了在这些企业 IT 风险的构成和各个企业管理 IT 风险的活动内容。本次研究提出了风险及风险管理能力的研究框架，为我们后来的研究奠定了基础。
- 由高德纳高管研究项目资助，在乔治·韦斯特曼主持下，对 134 家公司的调查。这项调研的统计数据使我们明白了四项 IT 风险最重要的驱动因素，以及什么可以使风险管理规则发挥作用。
- 乔治·韦斯特曼和理查德·亨特(Richard Hunter)共同主持的九家企业案例研究。它是我们为高德纳高管研究项目所做的主题报告的部分内容。通过与资助人和客户的共同努力，内容得到了扩展。透过这项调研，我们深化了认识和研究的实用观点。
- 我们多年在 IT 管理领域管理、研究和写作活动中收集的其他案例研究。中包含自己亲历的经验、访谈和系统研究，内容涉及 IT 的实施，经营的灵活性，过时遗留 IT 资产的转换，CIO 领导力等等。尽管在那时我们还不知道这些内容涉及到 IT 风险，但是随着我们对风险管理的认识，在我们的研究中它们变得紧密相关了。我们也认识到风险管理几乎能强化 IT 管理的各个方面。
- 2,000 多位 IT 主管、非 IT 主管和中层经理的观点意见。他们启发性的真知灼见是检验、提炼和改进我们认识的重要宝贵源泉。多年来，我们一直专注研究这些观点和理念，力图使它们成为真实世界实用的指针。

本书的读者

本书为来自经营业务部门和 IT 部门各类高管和经理提供了大量有用的观念、见解和案例。企业高管层和董事会成员可以利用这些观念和框架认识在管理 IT 风险中他们的责任，了解如何更好地履行他们重要的监督职责。CIO 可以利用本书填补与业务经营主管的鸿沟——使大家都能轻松自如的管理 IT 风险，同时兼顾

IT 与业务两个方面，建立切合实际的风险管理能力。

那些专项职能高管也能高效的利用本书。对于那些负责企业风险管理、安全、审计或合规管理的高管，他们会发现许多极有用的工具和案例，有助他们的风险管理活动（其中也包含 IT 风险管理）。对于其他一些专项高管——从经营业务领导到 IT 领导，无论是负责基础设施、安全、服务、应用开发，还是人力资源和关系管理——都能找到有价值的理念，辅助他们管理风险，理清他们管理风险的职责。最后，中层 IT 经理能够利用本书更好的理解 IT 与企业风险之间的关系，明了如何提高风险管理能力，帮助掌控企业风险状况。

致　谢

要感谢的人太多了，都不知从何说起。首先，我们要感谢许许多多的经理主管们，他们腾出宝贵的时间为我们谈论他们是如何管理 IT 风险的。许多麻省理工学院和高德纳之外的人——特别是戴维·福谢迪（David Fachetti）、查尔斯·加文（Charles Gavin）、迈克尔·哈特（Michael Harte）、罗比·希金斯（Robbie Higgens）、拉里·洛（Larry Loh）、科瓦夫·奥福里-博阿腾（Kwafo OforiBoateng）、里克·奥马丁（Rick Omartian）、汤姆·普林斯（Tom Prince）、帕特里克·珀塞尔（Patrick Purcell）、阿恩·斯基德（Arne Skeide）和卡尔·瓦克斯（Karl Wachs）——在设计研究构架，解析调研数据上发挥着非常重要的作用，还有部分人同样如此，但是为了保密的原因我们不能在此提及他们的名字。我们还要感谢许多参与了我们有关风险主题采访的人，他们完成了我们的调查表，阅读了报告，提出了许多宝贵的见解。

要感谢的还有我们的同事，谢谢他们持续不断的无私奉献和支持。乔治在麻省理工学院斯隆管理学院信息系统研究中心的同事——朱莉·科伊拉（Julie Coiro）、戴维·菲茨杰拉德（David Fitzgerald）、克里斯·福利亚（Chris Foglia）、尼尔斯·方斯塔德（Nils Fonstad）、查克·吉布森（Chuck Gibson）、杰克·罗克亚特（Jack Rockart）、珍妮·罗斯（Jeanne Ross）和彼得·韦尔（Peter Weill）——总是在贡献他们的良言与真知灼见。理查德在高德纳的同事〔包括高德纳高管研究项目研究团队和团队的领导马克·麦克唐纳（Mark McDonald）、戴夫·阿伦（Dave

Aron)、黛安娜·贝里(Diane Berry)、马库斯·布洛斯(Marcus Blosch)、芭芭拉·麦克纳林(Barbara McNurlin)、帕特里克·米汉(Patrick Meehan)、莉莉·莫(Lily Mok)、蒂娜农诺(Tina Nunno)、安德鲁·罗斯韦尔-琼斯(Andrew Roswell-Jones)、查克·塔克(Chuck Tucker)和安德鲁沃克(Andrew Walker)]和保密与安全委员会的成员。风险与防范研究委员会的成员[包括罗伯特·阿克利(Robert Akerley)、克里斯琴·伯恩斯(Christian Byrnes)、弗伦奇·考德威尔(French Caldwell)、里克德洛托(Rick deLotto)、特里·贾法里安(Trish Jaffarian)、阿维瓦·利塔(Avivah Litan)、里奇·莫古(Rich Mogull)、约翰·佩斯卡托雷(John Pescatore)、罗米利·鲍威尔(Romilly Powell)、保罗·普罗克特(Paul Proctor)、唐纳·斯科特(Donna Scott)和罗伯塔·威蒂(Roberta Witty)]为我们提供了丰富的研究报告和评论,支持我们的工作。在此我们还得感谢一些来自麻省理工学院硕士研究生的研究助理:维克拉姆·马希达(Vikram Mahidar)、米歇尔·萨拉查(Michele Salazar)、菲利普·孙(Philip Sun)、罗伯特·沃波尔(Robert Walpole)、和伦尼·泽尔策尔(Lenny Zeltser)。要致谢的还有凯瑟琳·安德森(Catherine Anderson)、杰姆·巴林顿(Jim Barrington)、布赖恩·克利里(Brian Cleary)、克里斯·柯伦(Chris Curran)、迈克尔·达菲(Michael Duffy)、迈克·弗卢顿(Mike Flouton)、巴德·马塔瑟(Bud Mathaisel)、彼得·摩根(Peter Morgan)、迈克尔·施拉格(Michael Schrage)、约翰·斯维克拉(John Sviokla)和瑞图·阿加瓦尔(Ritu Agarwal)教授、辛西娅·比思(Cynthia Beath)、温·金(Wynne Chin)、马尔科·兰瑟蒂(Marco Iansiti)、布莱克·艾夫斯(Blake Ives)、卡勒·吕蒂宁(Kalle Lyytinen)、沃伦·麦克法伦(Warren McFarlan)、瑞安·纳尔逊(Ryan Nelson)、杰夫·桑普尔(Jeff Sampler),谢谢他们的建议和为此项研究所做的投入。

最后,我们要感谢帮助我们成功写完这本书的朋友和同事。马克·麦克唐纳,鲍勃·杨(Bob Yang)和三位本书初稿的匿名评论者,他们为本书的最终定稿提出了非常宝贵的意见。从最初的设想到最终定稿,戴维·菲茨杰拉德、珍妮·罗斯和彼得·韦尔为本书的写作提出了不少金玉良言。还有,如果没有来自高德纳集团的希瑟·利维(Heather Levy)和哈佛商学院出版社的杰奎琳·墨菲(Jacqueline Murphy),就失去了他们专业的投入、努力和编辑的管理技巧,这本书也永远无法成功出版,所以也要向他们致谢。

乔治的个人补充

首先我得感谢我的妻子玛丽莲·奥古斯丁(Marilyn Augustyn)。对我来说,她是本书理念的生动证明:结婚就是一个风险,但是如果你管理得好,它会产生极大的价值回报。感谢你的爱、你的容忍、你的理解和在这漫长写作期间的帮助。还有我的孩子们,亨利(Henry)和克莱尔(Clare),他们为我带来新的生活,并且日复一日的保持着。最后,我要感谢我的父母、姊妹、朋友和导师,他们引导我走向正确的道路,鼓励我探索新生事物,享受其中所有的快乐。我永怀感激。

理查德的个人补充

我要感谢我的妻子,帕蒂(Patty)、我的孩子迪安(Dean)和苏珊(Susan);还有我的继子吉姆(Jim)和我的孙辈们伊莱亚斯·海斯(Elias Hayes)和塞缪尔·理查德(Samuel Richard),他们是我最重要、最好的人。我们承受着无常的风险,我们也沐浴在奖赏之中。

目录