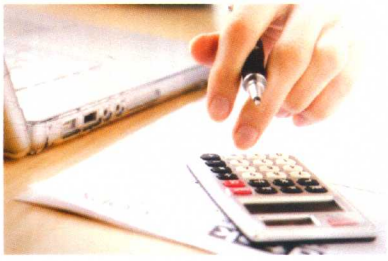
本书由扬州大学出版基金资助

信息系统安全投资策略及风险管理研究

Xinxi Xitong Anquan Touzi Celue Ji Fengxian Guanli Yanjiu



顾建强 著

西南财经大学出版社
Southwestern University of Finance & Economics Press
中国·成都

本书由扬州大学出版基金资助

信息系统安全投资策略及风险管理研究

Xinxi Xitong Anquan Touzi Celue Ji Fengxian Guanli Yanjiu

顾建强 著

西南财经大学出版社
Southwestern University of Finance & Economics Press

图书在版编目(CIP)数据

信息系统安全投资策略及风险管理研究/顾建强著. —成都:西南财经大学出版社,2016.11
ISBN 978-7-5504-2653-5

Ⅰ.①信… Ⅱ.①顾… Ⅲ.①企业管理—管理信息系统—投资风险—风险管理—研究 Ⅳ.①F272.7

中国版本图书馆 CIP 数据核字(2016)第 269191 号

信息系统安全投资策略及风险管理研究
顾建强 著

责任编辑:何春梅
责任校对:唐一丹 金欣蕾
封面设计:杨红鹰 张姗姗
责任印制:封俊川

出版发行	西南财经大学出版社(四川省成都市光华村街 55 号)
网 址	http://www.bookcj.com
电子邮件	bookcj@foxmail.com
邮政编码	610074
电 话	028-87353785 87352368
照 排	四川胜翔数码印务设计有限公司
印 刷	四川五洲彩印有限责任公司
成品尺寸	170mm×240mm
印 张	11.5
字 数	205 千字
版 次	2016 年 12 月第 1 版
印 次	2016 年 12 月第 1 次印刷
书 号	ISBN 978-7-5504-2653-5
定 价	58.00 元

前　言

随着计算机和网络技术的快速发展，信息系统正成为越来越多企业运营和管理的支撑工具，信息系统安全变得日渐重要。为了减少因安全事件导致严重损失的可能性，很多企业通常大量购买和运用防火墙、入侵检测系统等信息系统安全技术。然而，一个企业的信息系统安全不仅取决于自身的安全措施，而且与外部环境中的相关企业和黑客攻击方式等密切相关。因此，鉴于企业在相互依赖风险和黑客多样化攻击下的信息系统安全投资策略是企业信息系统运用过程中迫切需要解决的关键问题之一。同时随着信息系统安全管理服务和信息系统安全保险的出现，如何设计最优的激励机制，成为信息安全经济学的重要问题。本书对企业信息系统安全投资策略及风险管理的相关问题进行了研究。

首先，本书研究了信息系统相互关联下的企业信息系统安全投资策略，构建了博弈模型，讨论了关联企业的互联风险和信任风险对信息系统安全投资最优策略的影响，并对在非合作博弈条件下信息系统安全投资的均衡水平与社会最优的解决方案进行了比较。结果表明，互联风险往往引起企业信息系统安全投资率低下，而信任风险导致过度重视信息系统安全。在合作条件下，企业信息系统安全投资不一定随着互联风险和信任风险的增大而单调变化。此外，相对于社会最优水平，面临互联风险的企业是否过度投资完全取决于信任风险的大小。

其次，分别研究了黑客随机攻击和定向攻击情形下，基于微分博弈的信息

系统安全投资水平问题。研究了非合作博弈下信息系统安全投资的最优策略选择，在此基础上，讨论了安全投资效率、黑客学习能力、传染率、目标替代率以及企业的信息系统安全事件带来的损失等因素对信息系统脆弱性和最优信息系统安全投资水平的影响。在讨论了黑客随机攻击和定向攻击两种情形下两个企业合作博弈情形下最优策略选择的基础上，分别对比了非合作情形下的博弈均衡结果，得出企业在黑客随机攻击下维持低的投资率，在定向攻击下维持高的投资率的结论。发现了构建一种相互的支付激励机制可以消除企业投资不足或者过度的问题，从而使企业达到合作博弈下的最优投资水平，提高两个企业的联合收益。

再次，研究了信息系统安全外包背景下如何通过激励措施来协调信息系统安全管理服务商的投入水平，从而有效地控制信息系统安全风险的问题。考虑信息系统安全特征，提出了三种契约模型，即一般惩罚契约、部分外包契约和奖励-惩罚契约。在此基础上对不同契约模型的均衡结果进行了讨论和比较。研究结果表明，部分外包契约优于一般惩罚契约，但只有奖励-惩罚契约能够在诱导信息系统安全管理服务商最优投入的同时使委托企业获得最大的回报。此外，本书运用委托代理模型分析了信息系统安全外包中的双边道德风险问题，发现普通赔偿契约并不能阻止双边道德风险。因此，本书提出一种新的契约结构，即关系激励契约。通过研究发现，在一定的条件下，这种契约能够规避双边道德风险，促进双方投入最优投入水平，提升社会福利且委托企业获得更好的收益。

最后，结合风险管理理论和博弈理论研究企业采用信息系统安全保险时的投资策略及激励机制设计问题。一方面，为解决正向相互依赖下的信息系统安全投资不足问题，设计一种基于保险免赔额的信息系统安全投资激励机制。结果表明，适当的保险免赔额可以在一定程度上将这种负外部性内部化，进而改善企业安全水平，有效提高社会福利。另一方面，通过对比非合作博弈和社会最优下的自我防御投资和信息系统安全保险水平，提出相应的补贴协调机制。研究结果表明，当风险相互依赖程度趋于很小时，自我防御投资水平随其潜在

安全损失的上升而增大。企业在进行信息系统安全投资时往往会忽略对其他企业的边际外部成本或收益的影响，这种负外部性特征会导致企业自我防御投资和信息系统安全保险水平均低于社会最优化水平。政府通过补贴企业自我防御投资可以在一定程度上协调企业的风险管理决策，进而改善企业安全水平，有效提高社会福利。

本书得到了国家自然科学基金项目（71071033）、扬州大学出版基金项目、扬州社会科学重点项目等的支持。本书得以完成，需要感谢我的博士阶段导师，东南大学的梅姝娥教授，以及课题组的仲伟俊教授、硕士阶段的导师王锐兰教授。感谢东南大学经济管理学院的高星博士、南京工业大学经济与管理学院的赵柳榕博士、扬州大学商学院的薛庆根教授、营销与电子商务系的潘成云教授、电子商务研究中心的高功步教授的帮助！最后特别感谢我的父母，感谢您们多年来的辛勤培育和无私的爱！感谢我的妻子和儿子与我一起分享这几年生活的酸甜苦辣！

目　录

1 绪论

1.1 研究背景和问题提出

1.1.1 研究背景

随着信息技术的广泛运用和快速发展，大多数企业的日常运行和商业管理越来越依赖于信息系统的应用[1]，因此信息系统所承载信息和服务的安全性正变得越来越重要。信息系统在保密性、完整性、可用性等方面出现任何问题和故障都可能给企业运营以及资本市场声誉带来很大的影响[2]，甚至造成企业破产。当前信息化环境中，企业信息系统面临的各种黑客入侵事件越来越多，仅2014年以来，针对企业信息系统的严重的黑客入侵事件就发生了很多起，全球有超过上千次信息泄露事件（如图1.1所示）。2014年3月23日，携程网被曝出信息系统安全漏洞，将用于处理用户支付的服务接口开启了调试功能，使所有向银行验证持卡所有者接口传输的数据包均直接保存在本地服务器。同时因其支付日志存在安全漏洞，导致所有支付过程中的调试信息可被任意黑客读取，这些信息包括持卡人姓名、身份证、银行卡类别、银行卡号、CVV码，6位Bin。2014年4月7日，OpenSSL公布了在全球范围内得到广泛使用的SSL协议存在一个严重漏洞，该漏洞可令攻击者于远程轻易地获取服务器上所有的敏感信息，包括密码、安全数据和私人密钥。在漏洞披露的48小时之内，全

球最流行的网站和服务都迅速地打上了补丁。然而，攻击者在打补丁之前利用该漏洞获得的 SSL 密钥和证书还可以在超过 1 200 家企业的系统中使用，包括 VPN 及其他网络服务。2014 年 9 月，美国第二大家居建材用品零售商 Home Depot 遭遇 POS 机攻击，黑客使用名为 BlackPOS 的恶意软件发动了攻击，影响了全美国几乎所有 Home Depot 门店。根据涉及的零售店数量进行估计，受影响的客户数量可能以百万计，被盗的信息包含客户信用卡号码、邮政编码等数据，以及其他敏感的个人信息。其后几大零售商品牌被大肆报道其销售终端受破坏，导致整个零售业的核心被动摇。2014 年 11 月，黑客通过向索尼电影娱乐企业的电脑植入恶意软件，导致企业内部信息系统受到大规模的破坏而瘫痪，大量敏感信息和专有内容被泄露。2015 年，美国最大的医疗保险企业之一 Anthem 也遭到了黑客攻击，成为医疗行业中最大的网络攻击受害者。黑客窃取了客户的医疗识别号、社会保险号码、住宅地址和电子邮件地址，而这些信息可能会被用于医疗欺诈。

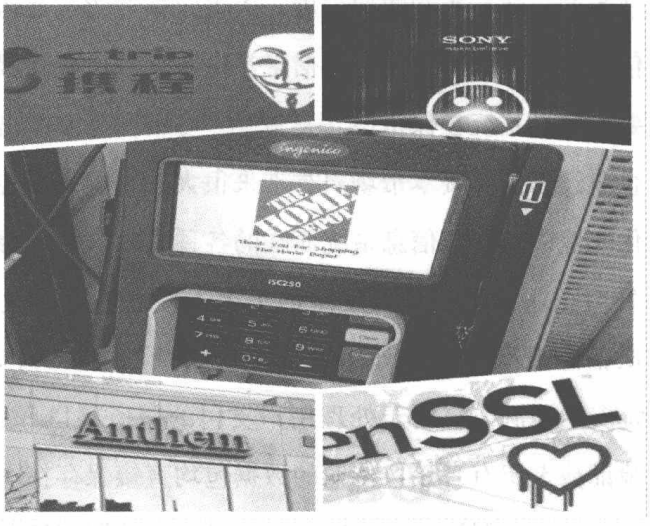


图 1.1　2014 年部分有影响力的信息系统安全事件

通过这些事件可以得到以下几点结论：

（1）黑客攻击和信息系统安全事件的发生已经成为常态。根据 Ponemon Institute 对美国 2013 年信息安全事件的调查研究[3]，发现这些被调查企业每周

都会遭受总数为122起的信息安全事件，平均而言，每个企业每周都会招致2起信息安全事件，与2012年相比有18%的提高。究其原因，一是目前的企业信息系统其实是非常脆弱的，从网络漏洞、系统漏洞到应用软件漏洞，甚至安全软件都会出现漏洞，且这些漏洞的发现有加快的趋势，因此导致攻击爆发时间变短。二是企业信息系统安全意识不足，缺乏相应的技术和人员支持，或者对信息系统安全投资不能进行有效的规划与管理。

（2）信息系统安全事件对企业造成的损失是非常巨大的。根据普华永道最新的全球信息安全状况调查[4]，全球信息系统安全事件正不断增长，无论信息系统安全事件起源于何处，其应对成本正在飙升。在中国内地和香港，2013年每家受访企业因信息系统安全事故导致的平均经济损失竟高达180万美元。同样来自Ponemon Institute对美国2013年网络犯罪的调查显示，样本中的60个企业平均每年因信息系统安全事件造成的损失从130万美元到5 800万美元不等，平均为1 160万美元。黑客一旦对银行、证券机构的计算机网络和信息系统进行攻击，往往会使金融机构蒙受重大损失，同时也给社会稳定带来极为不利的影响。

信息系统安全事件能给企业带来的损失主要有三种：

一是核心技术和竞争力的损失。对于高科技研发企业、设计企业等，专有技术、设计作品等是企业的核心竞争力，信息系统安全事故一旦发生，对它们往往产生致命的影响。比如某著名电子企业研发出一款新的电子产品投放市场，但是由于企业的核心技术被黑客获取转卖给另外一家企业，最后市场上出现了两款类似功能的产品，导致这家著名电子企业产品的竞争优势大打折扣。

二是社会信誉度损失。一旦发生信息系统安全事件，消费者和投资者会认为企业在信息系统安全管理上不负责任，而且这种不信任感会蔓延到企业各个方面，最终对企业形象、品牌忠诚度、资本市场筹资能力等造成不可挽回的损失。如2014年eBay旗下的服务器遭到了黑客的攻击，泄漏了用户的个人信息和账户密码，导致了很大的负面影响，令其在2014年第一季度客户大量减少。

三是直接经济损失。2015年，爱尔兰航空企业旗下的子企业瑞安航空的

银行账户遭到了黑客的攻击，被盗走500万美元。这个账户是瑞安航空用来为旗下飞机支付加油款项的基金账户，并且没有设置立即报警功能。IBM安全人员对此并不诧异，他们发现这次盗窃使用了专门的恶意软件，这类恶意软件问世以来已经从各家企业账户中盗走超过100万美元[5]。

（3）黑客的攻击主要是出于经济的目的。早期的黑客可能会以炫耀技术为目的，而现在黑客群体出现了分化，并开始大量出现以盈利为目的的攻击行为。这些攻击把企业信息系统作为目标，不经过授权就获取信息系统上存储的信息，对目标信息系统进行控制，或者改变数据的完整性以及信息系统的可用性，从而获取经济利益。特别是P2P行业日益火爆以来，相关企业遭遇黑客攻击的频率就大幅增加。据不完全统计，自2014年起，全国已有超过150家P2P平台由于黑客攻击造成系统瘫痪、数据恶意篡改等。而且随着信息技术的快速发展，黑客集团也逐渐形成了庞大、完整的集团和产业链。他们分工明确、无孔不入，不断地寻找各种漏洞并设计入侵/攻击流程，以期达到一定的经济目的（如图1.2所示）。

（4）黑客的攻击更加智能和隐蔽。随着时间的推移，黑客对信息系统的攻击已经变得更加复杂。从前的攻击需要黑客有相当高的专业技术水平和熟练的操作技能，现在，因特网中的黑客站点随处可见，黑客工具可以随意下载，很多脚本小子不需要自己发现系统漏洞，只需使用别人开发的黑客程序就能对企业信息系统进行攻击和破坏，这对信息系统安全构成了极大的威胁。低层次的黑客发动攻击所需要的技巧和知识并不是很高，但所造成的破坏性更大。另外黑客攻击的隐蔽性很强，攻击的证据没有专业知识很难获取，而实施恶意攻击的行为人却很容易毁灭这些证据。

信息系统安全威胁客观存在并不断增长，攻击技术、防御技术的改变和信息系统环境的变化（例如漏洞的不断发现）也都是日新月异。重要的是，在企业的运行和管理越来越依赖于信息系统的情况下，企业必须获得可靠的信息系统安全保障来确保组织的正常运行。面对越来越严峻的信息系统安全形势，企业等组织的常规做法是加大对信息系统安全的投入，购买和运用更多更先进

的信息安全设备和技术，如防火墙（firewall）、入侵检测系统（IDS）、虚拟专用网络（VPN）、防病毒软件、数据备份等。2015 年我国信息安全市场规模超过 25 亿美元，预计到 2019 年有望达到 48.2 亿美元，5 年复合增长率 14.5%，远高于全球信息安全市场增长速度。

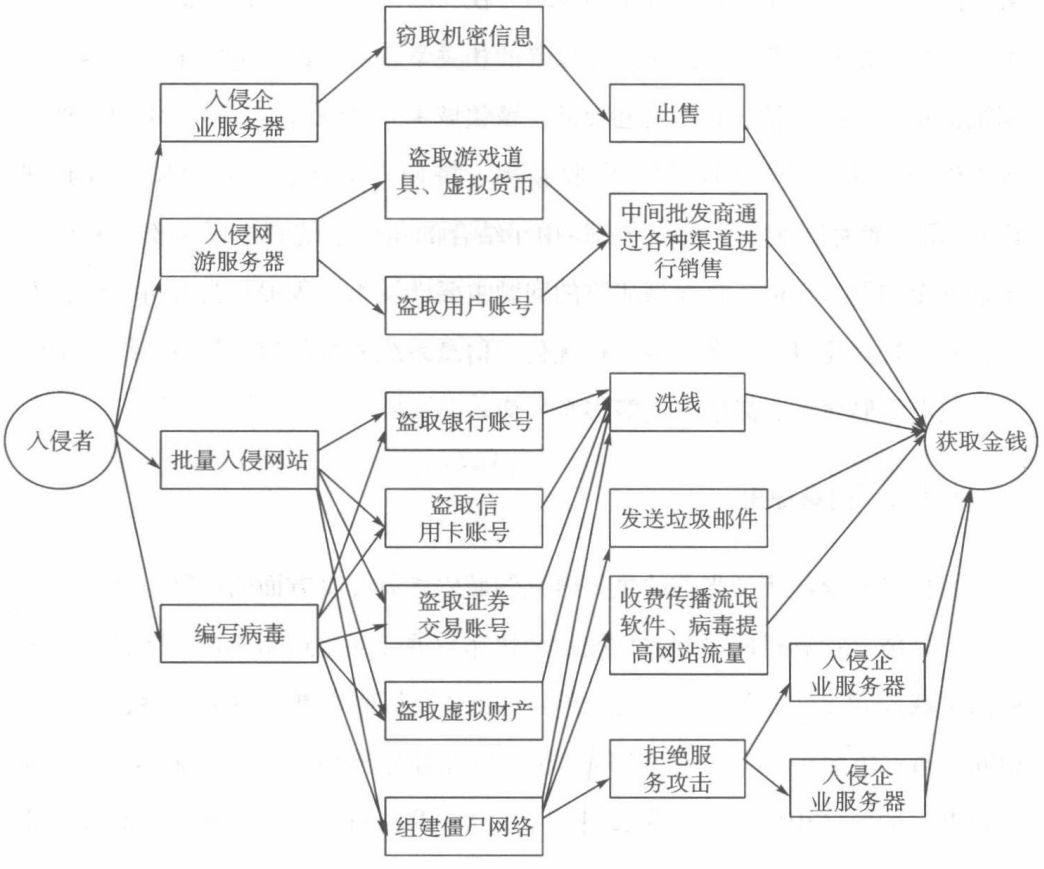


图 1.2　黑客/病毒产业链示意图

然而，最近的研究成果表明，并不是信息系统中的信息安全投资越大，运用的信息安全技术越多、越先进，其效果就一定越好[6]。特别需要强调的是，信息系统所处的网络环境不仅仅是由技术元素构成的，而是一个包含技术、管理者、黑客、风险关联企业、客户、信息系统安全管理服务商、保险企业等涉及多方利益相关者的庞大复杂经济社会系统。解决信息系统安全问题，仅仅依靠技术手段很难完全实现[7]，必须充分考虑各种影响因素和各类利益相关者的

策略或行为对信息系统安全的影响。当前，针对这些问题的研究形成了一个新的研究领域——信息安全经济学。虽然该研究领域出现较晚，但已经有一些成果发表在 *Science*，*Management Science*，*MIS Quarterly*，*Information Systems Research*，*Journal of Management Information Systems* 等国际顶级学术期刊上，国外著名高校如剑桥大学、加州大学伯克利分校、哈佛大学、卡内基梅隆大学、马里兰大学、德克萨斯大学达拉斯分校等的相关学者每年以专题学术会议的形式围绕信息安全经济学进行研讨和交流。该领域主要是综合运用经济学和管理学等理论与方法（如外部性、投资收益率、搭便车问题、道德风险、博弈理论），研究如何从制度设计和技术运用相结合的角度系统解决网络安全和信息系统安全问题。目前，该领域研究的问题主要涉及黑客入侵行为分析、信息安全技术配置优化以及安全投资策略优化、信息系统安全外包、信息系统安全保险、政府管制政策、激励机制等多个方面。

1.1.2 问题提出

在信息安全经济学当前的主要研究领域中，有几个方面的问题值得关注。

一是随着计算机网络和通信技术的快速发展，通过运用先进的信息技术来联系关联企业和整合供应链正成为各个行业的趋势，如电子数据交换（Electronic Data Interchange，EDI）、连续库存补充计划（Continuous Replenishment Program，CRP）、供应商管理库存（Vendor Managed Inventory，VMI）等的广泛运用使得企业与其上下游企业、甚至与竞争对手之间形成了紧密的联系和信息共享[8-12]。因此，关联企业信息系统的安全性直接影响一个企业信息系统的安全性。如果关联企业安全投资水平不高，共享信息不能得到有效的保护，企业提升自身信息系统安全性要付出的代价必然会提高[13-14]。例如一旦一个黑客成功入侵了网络化供应链中的任何一个企业，就很容易入侵供应链网络中的其他企业。因为在网络化供应链中，企业允许其协作企业直接通过其信任的方式来访问其相关信息，这也使一个企业的安全漏洞得以影响整个网络化供应链。

但是企业这种相互依赖性对企业的影响是和黑客攻击模式相关的，有时一个企业提升本企业的信息系统安全投资水平能够使黑客转而攻击另外的企业，从而降低其他企业的防御成功率。另外，也有不少研究认为黑客能够在资产相似企业中选择脆弱性高的或者资产价值大的目标进行攻击[15-16]。这种企业不同的相关作用在一定程度上必然影响企业之间的信息系统安全投资战略选择和风险管理方式。因此考虑黑客不同攻击模式下的信息系统安全投资策略和安全水平，以及研究企业的信息系统安全投资协调机制，是信息安全经济学研究领域的重点问题之一。

二是由于漏洞的不断发现和计算机病毒随时间快速扩散，形成了信息系统安全的动态环境。企业可以采用新的信息系统安全技术，黑客也可以通过学习获得新的攻击技术，所以企业在制定信息系统安全投资策略时需要充分考虑时间维度，即需要考虑企业和黑客所处网络环境随时间的动态变化以及系统脆弱性和黑客的学习能力等。这方面的研究一般可以运用微分博弈方法来进行分析，从而得到时间维度下企业信息系统安全投资策略。

三是信息系统安全管理服务商的出现和信息系统安全保险业务的发展促使企业有了新的风险管理模式和工具。所谓企业信息系统安全外包，简单来说，是指企业将全部或部分信息安全工作指定信息系统安全管理服务商完成的服务模式。由于信息系统安全管理服务商专门从事专业化的信息技术和信息系统安全工作，能够更加灵活地运用有限的预算资金，采购更加合适的设备，招募专业的技术人员和专家，提供模块化的可选择的服务，从而能使组织各种类型的信息资源在更低的成本上得到足够的安全保证。但是拥有这些优势的同时，也带来了新的问题。例如如何解决外包中普遍性的道德风险问题，如何结合技术模块和信息系统外包特征去考虑契约设计与风险控制问题，都值得去研究。

另外一个风险管理工具——信息系统安全保险则发展于英国。英国政府最近与私营部门合作向企业推广信息系统安全保险，确保信息系统安全保险成为企业 IT 安全的有力工具，帮助企业控制数据泄露风险。负责网络安全战略的英国内阁大臣弗朗西斯·莫德表示[17]，尽管保险不能代替安全的网络环境，