

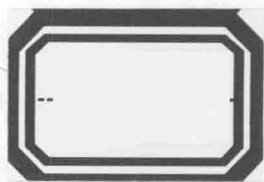
基于创新保护的 信息安全投资博弈研究

Research on Game of Information Security Investment
Based on Innovation Protection

孙薇 著



经济管理出版社
ECONOMY & MANAGEMENT PUBLISHING HOUSE



基于创新保护的 信息安全投资博弈研究

Research on Game of Information Security Investment
Based on Innovation Protection

孙薇 著



经济管理出版社
ECONOMY & MANAGEMENT PUBLISHING HOUSE

图书在版编目 (CIP) 数据

基于创新保护的信息安全投资博弈研究/孙薇著. —北京: 经济管理出版社, 2014.9
ISBN 978-7-5096-3266-6

I. ①基… II. ①孙… III. ①信息技术—高技术产业—投资—研究 IV. ①F49

中国版本图书馆 CIP 数据核字 (2014) 第 171483 号

组稿编辑: 张永美
责任编辑: 张永美
责任印制: 黄章平
责任校对: 超凡



出版发行: 经济管理出版社

(北京市海淀区北蜂窝 8 号中雅大厦 A 座 11 层 100038)

网 址: www.E-mp.com.cn

电 话: (010) 51915602

印 刷: 大恒数码印刷 (北京) 有限公司

经 销: 新华书店

开 本: 720mm×1000mm/16

印 张: 12.75

字 数: 236 千字

版 次: 2014 年 9 月第 1 版 2014 年 9 月第 1 次印刷

书 号: ISBN 978-7-5096-3266-6

定 价: 48.00 元

·版权所有 翻印必究·

凡购本社图书, 如有印装错误, 由本社读者服务部负责调换。

联系地址: 北京阜外月坛北小街 2 号

电话: (010) 68022974 邮编: 100836

《基于创新保护的信息安全投资博弈研究》一书是在辽宁大学商学院各位领导的积极鼓励下完成的，并且很多商学院同仁也给予了无私的帮助，在此一并深表感谢！

本书是在孙薇的博士论文基础上进一步加工、修改、提炼而成的。值此书稿付梓之际，深深感谢孙薇的博士生导师何德全院士、尤新刚教授和孔祥维教授，师恩难忘！

前言

Preface

创新是知识经济时代的重要特征,创新成果对企业的发展至关重要,因此,企业必须对创新成果的数字化载体加强保护。信息安全是当前世界范围内各种机构组织亟待解决的问题之一。与只关注信息安全的技术研究不同,信息安全问题实际上是包括技术、管理和法律在内的系统工程,其中的信息安全投资问题就是管理领域的重要问题之一。信息安全投资具有独特的策略依存性特点,这种策略依存性正是博弈论的基本特征,因而本书利用博弈理论研究组织的信息安全投资问题,为解决组织的信息安全投资难题提供了新的思路。

本书首先利用有限策略博弈分析了组织的信息安全投资决策问题,然后利用无限策略博弈分析了组织的信息安全投资的具体额度问题,并且考虑到现实社会中信息安全投资主体的有限理性问题,以及预测信息安全投资的长期稳定趋势的需要,利用演化博弈论研究了防守博弈和攻防博弈两种情况下信息安全投资的演化博弈。本书的主要研究内容及成果如下:

(1) 提出了组织信息安全投资决策的有限策略博弈分析方法,为组织正确制定信息安全投资决策提供决策支持。根据得益矩阵建立的两组织及多组织信息安全投资决策博弈模型,全面考虑了信息安全投资所产生的价值效益,不仅包括预防信息安全事故产生的直接价值效益,也考包括信息安全投资为组织带来的提升品牌价值、增加组织声誉等间接价值效益。对于两组织信息安全投资决策博弈模型,纯策略和混合策略纳什均衡分析的结果显现出两种纳什均衡分析的一致性,当信息安全投资成本较高时,惩罚变量的引入则有助于重新实现理想的纳什均

衡,并且,通过算例简要说明了两组织信息安全投资决策的博弈分析。在建立的多组织信息安全投资决策博弈模型中,对影响成本阈值的因素进行详细讨论,提出多组织信息安全投资的两项命题,得出信息安全投资成本对博弈均衡的影响规律,进一步寻找促使组织“投资”信息安全成为均衡结果的必要条件,并通过仿真进行验证分析。

(2)提出了组织信息安全投资额度的无限策略博弈分析方法,为组织合理确定信息安全投资的额度提供科学依据。信息安全投资不足无法保证足够的安全,而投资过多则会造成不必要的浪费,因而必须合理确定信息安全的具体投资额度。根据信息安全投资额度的策略依存性建立信息安全投资额度博弈模型,模型中关系参数的变化反映了两组织间博弈关系的变化。对于模型中关系参数取值的不同情况,根据反应函数法进行博弈的均衡分析。在攻防博弈关系情况下,推导出防守方均衡成本与关系参数相关关系的命题,并通过仿真进行验证。而且,通过算例简要说明了组织信息安全投资额度的博弈分析。

(3)提出了防守博弈和攻防博弈两种情况下信息安全投资的演化博弈分析方法,预测了博弈方有限理性下信息安全投资的长期稳定趋势。考虑到现实社会中信息安全投资主体的有限理性问题,以及预测信息安全投资的长期稳定趋势的需要,利用演化博弈论进行防守博弈与攻防博弈两种情况下信息安全投资的研究。在防守博弈下信息安全投资的演化博弈分析中,根据信息安全投资的演化博弈模型,通过复制动态分析防守博弈下信息安全投资演化博弈的进化稳定策略,并且通过 Repast 的多 Agent 仿真平台进行演化博弈的仿真验证,实验结果验证了演化博弈的进化稳定策略。对于攻防博弈下信息安全投资的演化博弈问题,首先建立信息安全攻防的博弈模型,分析防守方和攻击方的复制动态及进化稳定策略,进而根据攻防两群体复制动态的关系,得出攻防对抗的规律和长期稳定趋势,既从原理上解释了信息安全攻防循环的问题,也从演化博弈的分析中得出了解决信息安全问题的策略建议。

本书从博弈论的全新角度研究信息安全投资问题,为解决组织的信息安全投资难题进行了有益探索,取得了一些创新性的研究成果。本书的研究对这一前沿领域的开拓具有重要的理论意义,同时对于减少组织在信息安全投资问题中的盲目性、指导组织科学合理地进行信息安全投资具有重要的实践意义。

前言

Preface

Innovation is the characteristic of knowledge economic age, and innovation outcome is very important for enterprises, so enterprises should protect digital carrier of innovation outcome well. Information security is an urgent problem for all kinds of organizations all over the world. Information security is not just a research field of technology, but a systematical engineering of technology, management and law. Information security investment problem is the research field of management. The distinct characteristic of information security investment is strategy interdependence, and strategy interdependence is just the basic characteristic of Game Theory. This doctoral dissertation has made scientific researches on information security problem based on game theory, and provides new methods to solve information security problem for organizations.

This book analyzes information security investment decision problem of the organizations by finite strategy game first, then analyzes the investment quantity of information security by infinite strategy game. Also, in view of bounded rationality and the need to predict the long-term stable trend, this doctoral dissertation studies information security investment under defenders game and attacker-defender game by evolutionary game theory. The main works are as follows:

(1) The finite strategy game analysis method of information security investment decision for organizations is proposed, and it provides the decision support for the

correct information security investment. The information security investment decision game model is set up based on payoff matrix, and this game model contains all the value benefits of information security investment including the direct value benefits of preventing information security disaster and the indirect value benefits such as improving brand value and organization reputation. For information security investment decision game model between two organizations, the contrast of pure strategies and mixed strategies Nash Equilibrium shows the consistency of two analyses. In addition, when the information security investment cost is relatively high, the introduction of penalty parameter can achieve ideal Nash Equilibrium again. The example illustrates the information security investment game of two organizations. For the information security investment game model among organizations, the factors influencing cost threshold are discussed, and two propositions of information security investment are brought forward. The necessary conditions to achieve the equilibrium of investment are deduced, and the simulation analysis is made.

(2) The infinite strategy game analysis method of information security investment quantity for organizations is proposed, and it provides scientific reference for the proper investment quantity of information security. Insufficient investment of information security can not ensure enough security, and overabundant of investment induces the waste, so it is necessary to analyze the proper investment quantity of information security. The information security investment quantity game model is set up based on the strategy independence, and the relation parameter in the model reflects the game relation of the two organizations. According to the different value of the relation parameter, the equilibrium analysis is made based on reaction function method. In particular, for the attack-defence game, the correlation proposition of the defender's equilibrium cost and the relation parameter is set up, and verified by the simulation. The example illustrates the investment quantity game analysis.

(3) The evolutionary game analysis methods of information security investment under defenders game and attacker-defender game are proposed, solve the hard problem of bounded rationality of information security investment subject, and predict the long-term stable trend of information security investment. In view of the bounded

rationality of information security investment subject in the real world and the need to predict the long-term stable trend of information security investment, the evolutionary game researches of information security investment under defenders game and attacker-defender game are made in order to strengthen the reality basis of information security investment game. In the evolutionary game analysis of information security investment under defenders game, based on the evolutionary game model of information security investment, Evolutionary Stable Strategy is analyzed by Replicator Dynamics. The Repast simulation on the multi-agent platform verifies the Evolutionary Stable Strategy. For the evolutionary game of information security investment under attacker-defender game, the attacker-defender game model of information security is set up, and the Replicator Dynamics and Evolutionary Stable Strategy are analyzed. The law and long-term stable trend of attack and defence are studied based on the relation of Replicator Dynamics of the attacker colony and Replicator Dynamics of the defender colony. The research results explain the circle of attack and defence in information security, and put forward the strategy suggestions to settle information security problem.

This doctoral dissertation has made scientific researches on information security problem for organizations from the new angle of game theory, explored the hard problem of information security investment, and achieved some innovative research results. This doctoral dissertation has important theoretical significance for this new research field, and also has important practical significance to reduce the blindness of the investment, and to direct information security investment scientifically.

目 录 Contents

第 1 章 绪 论 / 001

- 1.1 知识经济时代中的创新保护 / 001
- 1.2 信息安全对创新保护的重要性 / 003
- 1.3 博弈论的理论基础 / 011
 - 1.3.1 博弈论的创立及发展 / 011
 - 1.3.2 博弈论的基本概念 / 016
 - 1.3.3 基本的博弈类型及其均衡 / 018
- 1.4 本书的主要研究内容和创新点 / 024
 - 1.4.1 本书的主要研究内容 / 024
 - 1.4.2 本书的创新点 / 026
 - 1.4.3 本书的结构安排 / 026

参考文献 / 027

第 2 章 创新保护与大企业竞争力 / 031

- 2.1 知识经济时代的创新 / 031
- 2.2 创新过程与创新成果的保护 / 036
- 2.3 创新保护与知识产权 / 040
- 2.4 创新保护对大企业竞争力的提升作用 / 045

参考文献 / 052

第3章 创新保护的利剑——信息安全 / 053

3.1 创新保护的方式 / 053

3.2 信息安全投资对创新成果的有效保护 / 055

3.3 国内外相关研究的最新进展 / 057

3.3.1 信息安全投资的研究进展 / 057

3.3.2 博弈论应用的研究进展 / 062

3.3.3 博弈论应用于信息安全投资问题的研究进展 / 064

3.3.4 国内外相关研究小结 / 065

参考文献 / 067

第4章 创新保护中信息安全投资决策的博弈分析 / 073

4.1 创新保护中信息安全投资决策博弈模型的建立与基本假设 / 073

4.1.1 两组织信息安全投资决策博弈模型 / 074

4.1.2 多组织信息安全投资决策博弈模型 / 075

4.2 创新保护中信息安全投资决策博弈的均衡分析 / 076

4.2.1 两组织信息安全投资决策博弈的均衡分析 / 076

4.2.2 多组织信息安全投资决策博弈的均衡分析 / 078

4.3 创新保护中两组织信息安全投资决策博弈的算例及应用分析 / 079

4.4 创新保护中多组织信息安全投资决策博弈的仿真分析 / 081

4.5 小结 / 084

参考文献 / 085

第5章 创新保护中信息安全投资额度的博弈分析 / 087

5.1 创新保护中信息安全投资额度博弈模型的建立与基本假设 / 087

5.2 创新保护中信息安全投资额度博弈的均衡分析 / 088

5.2.1 $a=1$ 时的投资额度博弈均衡 / 089

5.2.2 $0 < a < 1$ 时的投资额度博弈均衡 / 091

5.2.3 $a=0$ 时的投资额度博弈均衡 / 092

- 5.2.4 $-1 < a < 0$ 时的投资额度博弈均衡 / 093
- 5.2.5 $a = -1$ 时的投资额度博弈均衡 / 094
- 5.3 创新保护中信息安全投资额度博弈均衡的仿真分析 / 096
- 5.4 创新保护中信息安全投资额度博弈的算例及应用分析 / 097
 - 5.4.1 $a = 1$ 时的投资额度博弈均衡 / 098
 - 5.4.2 $0 < a < 1$ 时的投资额度博弈均衡 / 099
 - 5.4.3 $a = 0$ 时的投资额度博弈均衡 / 100
 - 5.4.4 $-1 < a < 0$ 时的投资额度博弈均衡 / 100
 - 5.4.5 $a = -1$ 时的投资额度博弈均衡 / 101
- 5.5 小 结 / 102
- 参考文献 / 102

第 6 章 防守博弈下基于创新保护的信息安全投资的演化博弈分析 / 103

- 6.1 防守博弈下的信息安全投资博弈模型 / 104
- 6.2 防守博弈下信息安全投资演化博弈的复制动态 / 105
- 6.3 Repast 的仿真模型 / 107
 - 6.3.1 复杂系统仿真 / 107
 - 6.3.2 基于 Agent 的系统仿真 / 108
 - 6.3.3 Agent 仿真工具 / 111
 - 6.3.4 Repast 仿真平台 / 117
- 6.4 防守博弈下信息安全投资演化博弈的进化稳定策略及仿真 / 122
 - 6.4.1 $x_a^* \leq 0$ 时的进化稳定策略及仿真 / 122
 - 6.4.2 $x_a^* \geq 1$ 时的进化稳定策略 / 126
 - 6.4.3 $0 < x_a^* < 1$ 时的进化稳定策略 / 129
- 6.5 防守博弈下引入惩罚变量的信息安全投资演化博弈 / 133
 - 6.5.1 $x_a^* \leq 0$ 时的进化稳定策略分析 / 134
 - 6.5.2 $x_a^* \geq 1$ 时的进化稳定策略分析 / 135
 - 6.5.3 $0 < x_a^* < 1$ 时的进化稳定策略分析 / 136
- 6.6 小 结 / 137
- 参考文献 / 137

第7章 攻防博弈下基于创新保护的信息安全投资的演化博弈分析 / 141

7.1 信息安全攻防对抗的博弈模型 / 141

7.2 完全理性下信息安全攻防对抗的博弈分析 / 142

7.2.1 完全理性下信息安全攻防对抗的均衡分析 / 142

7.2.2 完全理性下引入防守方惩罚变量的攻防对抗博弈分析 / 143

7.2.3 完全理性下引入攻击方惩罚变量的攻防对抗博弈分析 / 144

7.3 有限理性下信息安全攻防演化博弈的复制动态 / 145

7.4 有限理性下信息安全攻防演化博弈的进化稳定策略 / 146

7.5 有限理性下攻防两群体复制动态的关系和稳定性分析 / 149

$$7.5.1 \quad \begin{cases} 0 < \frac{C-I}{2E} < 1 \\ 0 < \frac{E-K}{E} < 1 \end{cases} \quad \text{时两群体复制动态的关系和稳定性分析 / 150}$$

$$7.5.2 \quad \begin{cases} \frac{C-I}{2E} \leq 0 \\ 0 < \frac{E-K}{E} < 1 \end{cases} \quad \text{时两群体复制动态的关系和稳定性分析 / 151}$$

$$7.5.3 \quad \begin{cases} \frac{C-I}{2E} \geq 1 \\ 0 < \frac{E-K}{E} < 1 \end{cases} \quad \text{时两群体复制动态的关系和稳定性分析 / 152}$$

$$7.5.4 \quad \begin{cases} 0 < \frac{C-I}{2E} < 1 \\ \frac{E-K}{E} \leq 0 \end{cases} \quad \text{时两群体复制动态的关系和稳定性分析 / 153}$$

$$7.5.5 \quad \begin{cases} \frac{C-I}{2E} \geq 1 \\ \frac{E-K}{E} \leq 0 \end{cases} \quad \text{时两群体复制动态的关系和稳定性分析 / 154}$$

$$7.5.6 \quad \begin{cases} \frac{C-I}{2E} \leq 0 \\ \frac{E-K}{E} \leq 0 \end{cases} \quad \text{时两群体复制动态的关系和稳定性分析 / 154}$$

7.6 小 结 / 157

第 8 章 总结与展望 / 159

8.1 总 结 / 159

8.2 展 望 / 160

附录 1 演化博弈仿真的 Java 代码 / 163

附录 2 Repast 在 Eclipse 中的配置与调试 / 179

附录 3 信息安全投资演化博弈仿真流程 / 183

第1章

Chapter One

绪 论

1.1 知识经济时代中的创新保护

21 世纪是知识经济时代。知识经济也称智能经济，是建立在知识和信息的生产、分配和使用基础上的经济，主要以知识为基础，是极具生命力的新型经济形态，也是与农业经济和工业经济相对应的一个概念。

知识经济有广义与狭义之分^[1]。广义的知识经济是指一种经济形态或经济时代，这种经济形态中还有农业部门和工业部门，只不过是以知识产业部门为主，且工农业都相当程度地知识化了。狭义的知识经济是指知识产业，这类似于农业经济特指农业部门的经济，工业经济特指工业部门的经济。

世界经合组织（OECD）在 1996 年的年度报告中提出了“以知识为基础的经济”的概念，并认为“这种经济直接依赖于知识和信息的生产、分配及使用”。不难看到，“知识经济”只不过是“以知识为基础的经济”的简称。

在 OECD 的定义中将“知识”与“信息”并列，强调两者的生产、分配与使用都属于知识经济的范畴。相反，不是直接与知识和信息的生产、分配和使用有关的经济，不属于知识经济的范畴。

知识经济表达了知识作为生产要素的重要性^[1]，它与以劳动为基础的经济、以资本为基础的经济一样，都属于按生产要素划分的经济形态。从人类经济发展

史来看,土地、劳动、资本、知识等都是影响经济增长的要素,通过一组生产要素的投入,就可能实现一定数量和质量的产品的产出,达到经济增长的目的,这是所有经济形态下共同的经济增长过程。任何一种经济形态都存在劳动与资本对经济增长的作用,也存在知识对经济增长的作用。但在不同时代,各种生产要素对经济增长的影响程度不同,这成为划分经济形态的标准之一。与其他经济形态不同的是,“知识经济”是“知识”成为经济增长的“主导生产要素”的经济形态。

任何一种产业部门也都同时存在上述各类生产要素的作用。以知识为基础的经济在各个行业中皆有,仅仅是在不同行业中的比重、程度不同罢了^[1]。如OECD在1996年的年度报告中进一步解释了“以知识为基础的经济”的两个主要组成部分:一是制造业中的高技术产业,包括计算机、电子和航天行业等,过去10年中,这些行业的产出和就业增长很快,OECD成员国的高技术产业在制造业和出口中的份额翻了一番多;二是知识密集型的服务部门,如教育、通信、信息服务业等的发展。OECD估计,目前其主要成员国国内生产总值的50%以上是以知识为基础的。但是,由于“以知识为基础的经济”目前尚未与各国及国际统计口径完全接轨,因此,OECD认为“50%以上”只是一个“估计”数。

知识经济是人类知识,尤其是科学技术方面的知识积累到一定程度,并且在经济发展中的作用增加到一定阶段的历史产物,同时,知识经济更是新的信息革命导致知识共享以高效率产生新知识的经济形态。

知识经济使得知识要素上升到社会经济发展的基础地位,知识成为最重要的资源,在知识基础上形成的科技实力就成为最重要的竞争力。国家的振兴、民族的发展、企业的成功都在很大程度上依赖于对知识的掌握和创造性的开拓与应用,对于知识的生产、学习和创新已经成为人类最重要的活动之一,知识也相应成为时代发展的主要推动力。

OECD在《以知识为基础的经济》的报告中详细指出,知识经济是建立在知识的生产、分配和使用基础上的经济,其中的知识指人类迄今为止所创造的所有知识,最重要的就是科学技术、管理及行为科学知识。

正如种植和养殖方面的技术革命将人类带入农业经济时代,蒸汽机和电气方面的技术革命推动人类进入了工业经济时代,信息技术革命则是带领我们人类进入了崭新的知识经济时代。知识经济的基础实际上是信息技术,以数字化、网络

化和信息化为特征的新的信息革命为人类信息共享,高效率地生产出新知识,大幅度提高知识生产的效率,极大地推动了人类社会进入知识经济时代的步伐。可见,知识经济的关键就是知识生产率,也就是创新能力。

知识创新^①是人类经济和社会发展的重要动力源泉,建设国家创新体系和提高全社会创新意识和国家创新能力,是实现中国跨世纪发展之路的重中之重。然而,知识经济时代下的创新成果可学习性极强,如果没有适当的保护机制,一旦创新成果形成电子文档等形式保存下来,很有可能因为信息安全问题导致创新成果的泄露,所有创新的前期投资都会付诸东流,因此,保护创新成果是知识经济社会中极为重要的问题,从企业的视角来看,创新成果的保护是对创新成本的保障,也是对企业竞争力的重要保护,从社会的宏观视角来看,这也是社会进步必不可少的重要环节。

1.2 信息安全对创新保护的重要性

在这个知识经济的新时代,所有创新成果一旦形成电子文档等信息形式进行保存,就会涉及对其进行保护的重要问题。信息安全不仅关系到企业创新成果的保护问题,更关系到经济的发展、社会的稳定、政权的巩固、民族的兴衰和国家的存亡。因此,信息安全不仅是企业安全的关键环节,也已成为国家安全的重要保障。

当今社会信息安全的国际环境和国内环境都发生了巨大变化:计算机用户爆炸式增长,互联网迅速普及,信息空间作为组织、经济、政治、社会和战争的运作环境而出现,数字融合使信息能以任何形式和方式进行组合、改变和再利用,全球互联使计算机系统日益控制全面的基础设施。在这个信息环境中,所有国家、组织和个人都生活在一个每天都在加强联系的世界中。特别地,电子商务、

^① 知识创新主要指通过基础研究和应用研究等,获得新的基础科学和技术科学知识等的过程。