

不同攻击类型下风险厌恶型企业信息安全投资策略

潘崇霞, 仲伟俊*, 梅姝娥

(东南大学经济管理学院, 江苏 南京 211189)

摘要: 基于期望效用理论, 通过建立两企业的投资博弈模型, 并考虑随机攻击和定向攻击两种情形, 对风险厌恶型企业的信息安全投资决策进行了研究, 给出了信息共享情况下企业的最优信息安全投资策略, 并分析了风险厌恶水平, 黑客攻击概率与网络暴露程度等相关因素对最优安全投资策略的影响. 研究表明, 随机攻击情形下, 当企业极度厌恶风险时, 企业最优信息安全投资随着风险厌恶水平的增加而增加; 当企业轻微厌恶风险时, 若潜在损失较小或者黑客攻击概率较小或者网络暴露程度太高或者太低时, 企业的最优信息安全投资随着风险厌恶水平的增加而减小, 若潜在损失较大或者黑客攻击概率较大或者网络暴露程度中等时, 最优信息安全投资随着风险厌恶水平的增加而增加. 而定向攻击情形下, 当企业极度厌恶风险时, 企业最优信息安全投资随着风险厌恶水平的增加而减小.

关键词: 信息安全投资; 风险厌恶型企业; 随机攻击; 定向攻击; 信息共享

中图分类号: TP309

文献标识码: A

文章编号: 1000-5781(2019)04-0497-14

doi: 10.13383/j.cnki.jse.2019.04.006

Information investment strategies for two risk-averse firms under heterogeneous attacks

Pan Chongxia, Zhong Weijun*, Mei Shue

(School of Economics & Management, Southeast University, Nanjing 211189, China)

Abstract: This paper investigates information security investment decisions in consideration of opportunistic attacks and targeted attacks by establishing an investment game between two risk-averse firms based on expected utility theory. It gives the optimal security investment strategies under the condition of information sharing and analyzes the influences of relevant factors such as risk aversion degree, the hacker's attack probability and network exposure on the optimal security investment strategies. It is found that the optimal information security investment increases with the risk-aversion coefficient when risk-averse firms defend against opportunistic attacks and the risk-aversion coefficient is very high. When the risk-aversion degree is low, or the potential loss remains small, or the attack probability remains small, or either the network exposure is very high or very low, the optimal information security investment is decreasing with the risk-aversion coefficient; otherwise, the optimal information security investment is increasing with the risk-aversion coefficient when the potential loss remains large, or attack probability remains high, or network exposure is medium. On the contrary, the optimal information security investment is decreasing with the risk-aversion coefficient when risk-averse firms are faced with targeted attacks and they are extremely risk averse.

Key words: information security investment; risk-averse firm; opportunistic attack; targeted attack; information sharing

收稿日期: 2017-05-11; 修订日期: 2018-07-19.

基金项目: 国家自然科学基金资助项目(71371050).

*通信作者

1 引言

目前,信息安全投资研究受到国内外学者的广泛关注,企业信息安全投资(本论文所使用信息安全的定义是对通过互联网或任何其他计算机网络传输信息的保护,可以与网络安全交互使用)主要包括单个或多个企业的信息安全投资决策,需要考虑网络系统的特点、黑客的行为、企业与企业之间的博弈、企业与黑客之间的博弈等.单个企业的收益或效用需要考虑企业决策者的偏好、企业的安全投资成本、投资分配和潜在损失等;多个企业的收益或效用除了需要考虑单个企业的因素之外,还需要考虑企业之间的博弈、安全信息共享、相互关联性和投资外部性等;研究黑客的行为需要考虑黑客的入侵概率、入侵收益、攻击成本、黑客的攻击类型和黑客的攻击偏好等;网络系统的特点则需要考虑网络系统的脆弱性、网络系统的结构等因素.

在信息安全投资策略研究中, Gordon等^[1]对网络安全投资中所使用的Gordon-Loeb模型在实际应用中的设置作了进一步研究,为企业选择合理的网络安全投资水平提供了有益的指导. Gordon等^[2]研究了网络安全投资的经济分析模型,用于评价政府激励或调节措施对弥补私营企业网络安全投资不足的影响,指出政府激励或调节措施能否弥补私营企业网络安全投资不足取决于以下两点,一是私营企业是否进行了网络安全的最优混合投入,二是私营企业是否愿意提高网络安全投资. Nagurney等^[3]建立了供应链中多个零售商与多个消费者的期望效用(期望利润)模型,在考虑网络脆弱性的情况下对网络安全投资策略进行了研究. Nagurney等^[4]开创性地建立了供应链网络中非线性资金预算约束下零售商与市场消费者之间的网络安全投资博弈模型,提出了一个新的替代方程及其算法,这个算法可以在每次的迭代中产生有关产品交易、安全水平与预算约束相关的拉格朗日乘数的封闭式表达式,从而扩大了我们对于零售商、需求价格函数、经济损失与网络安全投资的理解. Nagurney等^[5]提出了三个有关多个企业的网络安全投资模型,分别在合作和竞争的条件下对这三个模型的期望效用进行了均衡分析,对网络脆弱性如何影响网络安全投资水平也进行了研究.熊强等^[6]分析了供应链中两种企业的信息资产价值、网络脆弱性、共享成本与互补性等因素对信息安全投资决策的影响.

对安全事件信息进行共享受到各国政府与公共组织的鼓励,信息共享已成为信息安全投资策略研究的重要问题. Gordon等指出信息共享可以帮助企业减少信息安全投资,提高信息安全水平,有利于提高社会的整体福利^[7]. Gordon等^[8]从实物期权的角度讨论了信息共享对信息安全投资的影响,指出当信息安全投资不确定性提高时,信息安全投资的延期期权价值增加,当信息共享达到一定水平时,可以减少信息安全投资的不确定性. Gao等^[9]研究了两个产品互补型企业在信息共享下的安全投资博弈,重点讨论了两企业独立进行投资决策的最优投资策略,并与两个产品替代企业的投资策略研究进行了比较,指出没有必要提倡社会管理者对企业信息安全投资进行过多干预.在文献[10]中, Gao等采用Gordon-Cavusoglu入侵概率函数(由Cavusoglu等^[11]在Gordon-Loeb模型的基础上经过改进的入侵概率函数)分别对两个企业信息共享情况下的安全投资进行了分析.论文首先分析了两个企业独立进行决策时,信息共享、黑客攻击、企业安全投资与入侵概率的均衡,并与以下三种情况的均衡进行对比:社会控制企业的安全投资、社会控制企业的信息共享、社会既控制企业的安全投资又控制其信息共享. Gal-Or等^[12]对两个竞争企业的信息共享进行了Bertrand博弈分析,研究发现,两企业的产品替代程度越高,信息共享就越有价值. Schechter等^[13]采用经济威胁模型研究了一个企图利用网络脆弱性进入对手信息系统的行为,研究指出,信息共享可以阻止对手入侵,间接提高安全技术的效率.杨丰梅等^[14]通过建立演化博弈模型对电商平台下的信用信息共享策略进行了研究.张子辰等^[15]通过建立Stackelberg博弈模型及合作博弈模型,在考虑信息共享与广告效应的情况下对不确定条件下的制造商和零售商的最优投资策略进行了研究.

为方便研究,学者一般把黑客的攻击类型分为随机攻击和定向攻击两种类型.美国信息安全研究机构Ponemon和Richardson计算机安全机构对这两种类型的攻击进行了定义,指出随机攻击并不针对特定的目标进行攻击,只是对可以连接的、容易访问的节点进行攻击,采取的主要方式为蠕虫病毒、间谍软件、钓鱼

软件和垃圾邮件等,而定向攻击则是针对特定的信息系统进行攻击,用于盗取数据或者进行破坏,采取的主要方式是拒绝服务和定向入侵等. Gao等^[16]讨论了两个竞争企业与一个黑客在两种攻击类型下的安全投资策略,黑客采用定向攻击比采用随机攻击能够获得更高的期望收益. 在两种攻击类型下,安全等级要求有时候可以较大程度改变安全投资策略. 假设安全等级要求是内在变量,当两企业的竞争比较激烈时,在定向攻击与随机攻击时,两企业都愿意保持严格的安全等级管理要求,当两企业的竞争比较温和时,两企业都愿意保护宽松的安全等级要求. Huang^[17]采用经济学模型研究了单个企业在同时面对多种攻击类型和一定预算下的信息安全投资及其投资分配策略,文献重点分析了随机攻击和定向攻击两种攻击类型.

有关企业决策者风险偏好的研究, Gordon等^[18]在考虑信息系统脆弱性和信息资产潜在损失的情况下对安全投资策略进行了研究,文献假设决策者的偏好是风险中立的,指出当信息系统的脆弱性增大时不必一定增大投资. Huang等^[19]研究了单个企业风险厌恶型决策者的信息安全投资策略,考虑了企业同时面对随机攻击和定向攻击两种攻击类型,对信息系统的脆弱性、潜在损失、风险厌恶系数、投资效率等与最优安全投资的关系进行了讨论. 赵柳榕等^[20]分析了黑客和企业的风险偏好对两种技术配置策略的影响,指出当公司的期望成本较低时风险中立型公司更易被入侵,当公司的期望成本较高时风险厌恶型公司更易被入侵,当黑客的期望收益较低时风险厌恶型黑客被检测的概率最大. 方玲等^[21]基于组织与黑客的风险偏好对信息系统安全技术选择与配置策略进行了研究,指出组织在黑客期望收益非常低时对风险厌恶型黑客的人工调查率更高,而在黑客期望收益非常高时对风险中立型黑客的调查率更高,黑客在组织人工调查成本较低时更倾向于入侵风险中立型组织.

综上所述,文献[1-6]基于Gordon-Loeb安全投资模型和供应链网络中的信息安全投资模型,对网络脆弱性、政府激励、需求价格、合作与竞争环境等因素对信息安全投资策略的影响进行了分析. 文献[7-15]侧重研究信息共享对企业投资策略的影响,没有考虑黑客的攻击类型和决策者风险偏好,文献[16,17]主要分析了单个企业面对多种攻击类型时的信息安全投资策略,没有考虑信息共享与决策者风险偏好等因素. 文献[18-21]考虑了企业和黑客的风险偏好对信息安全投资策略的影响,虽然同时考虑了随机攻击和定向攻击两种攻击类型,但没有定量分析两种攻击类型及其相关因素(如网络暴露程度、黑客攻击概率、两个企业的投资博弈、信息共享等)对企业信息安全投资策略的影响. 基于已有的文献研究,本文构建了期望效用模型,同时考虑了随机攻击与定向攻击两种攻击类型、信息共享、决策者风险偏好、两企业之间的投资博弈等因素,分别对随机攻击与定向攻击情形下的两个风险厌恶型企业的信息安全投资策略进行了研究.

2 两种攻击类型下的信息安全投资策略模型

2.1 参数描述

假设市场上只有两个寡头企业,企业1与企业2,企业1拥有的总价值为 w_1 ,企业2拥有的总价值为 w_2 . 在信息安全投资中,企业1对自身的信息安全投资为 s_1 ,企业2对自身信息安全投资为 s_2 ,在两企业进行信息共享的情况下,企业1进行的安全投资效果相当于 $s_1 + \lambda_2 s_2$,企业2进行的安全投资效果相当于 $s_2 + \lambda_1 s_1$,其中 $\lambda_1 \in [0, 1]$ 和 $\lambda_2 \in [0, 1]$ 分别是企业1与企业2的信息共享系数. 两个企业的决策者属风险厌恶型,并根据期望效用理论进行决策,当他们进行信息安全投资决策时,采取最优安全投资以最大化自己的期望效用. 效用函数为企业价值 w 的增函数^[22,23],指数效用函数被广泛应用于保险、经济领域等的投资决策^[24,25],根据Pratt等^[26]的定义,指数效用函数 $u(w) = \beta - \alpha e^{-\alpha w}$ 中的风险厌恶型系数 $\alpha \geq 0$ 是常量, β 是常量. 当企业被黑客入侵时,给企业造成的潜在损失为 L ,这些潜在损失可以有形资产如钱、信息资产等,也可以是无形资产,如企业的名誉或者市场消费者对企业网络安全的信任等. 企业价值为总价值 w 减去安全投资 s 和潜在损失 L 为 $w - s - L$,当企业没有被入侵时,企业价值为总价值 w 减去安全投资 s ,即 $w - s$,如表1所示.

由表1可知企业的期望效用函数为 $EU = \rho(\beta - \alpha e^{-\alpha(w-s-L)}) + (1 - \rho)(\beta - \alpha e^{-\alpha(w-s)})$,其中 ρ 为黑客入侵概率. 一般情况下,企业常常面临随机攻击与定向攻击两种攻击类型. 在文献[17]中Huang等对这两种

攻击类型的入侵函数进行了明确定义,对随机攻击类型的入侵概率定义为 $\rho = \xi c^{ks+1}$,把定向攻击类型的入侵概率定义为 $\rho = \xi c/(ks+1)$,当企业的投资为0时, $\rho_i(\xi, c, 0) = \xi c$. 其中, ξ 表示黑客的攻击概率,取值范围 $[0, 1]$,反映了企业的网络系统遭受攻击的概率. 企业网络暴露程度 c ,取值范围 $[0, 1]$,反映了企业网络系统与其他企业的联接程度和开放程度,网络暴露程度的高低取决于企业网络系统的商业要求和安全技术特性,与之联接的企业网络结点越多,网络暴露程度越高. s 表示企业进行的信息安全投资, k 表示企业进行信息安全投资的效率. 相关参数和变量见表2.

表1 企业期望效用表
Table 1 Firm's expected utility

参数	取值
被入侵概率	ρ
企业的价值	$w - s - L$
企业的效用	$\beta - \alpha e^{-\alpha(w-s-L)}$
	$1 - \rho$
	$w - s$
	$\beta - \alpha e^{-\alpha(w-s)}$

表2 符号表
Table 2 Parameters' description

符号	表示意义
L	黑客入侵对企业造成的潜在损失
s_i	企业 <i>i</i> 的信息安全投资水平 ($i = 1, 2$)
w	企业拥有的总价值
$\lambda_i \in [0, 1]$	企业 <i>i</i> 的安全信息共享率
$\alpha \geq 0$	风险厌恶系数
β	风险厌恶函数中的一个常数
$k_i \in [0, 1]$	企业 <i>i</i> 的安全投资效率
$\xi \in [0, 1]$	黑客攻击概率
$c \in [0, 1]$	网络暴露程度
ρ_i	黑客对企业 <i>i</i> 网络系统的入侵概率函数
$u(w)$	期望效用函数, 价值 <i>w</i> 的函数

2.2 随机攻击情形下的信息安全投资策略

随机攻击情形下,当两企业进行信息共享时,企业1进行的安全投资效果相当于 $s_1 = s_1 + \lambda_2 s_2$,企业2进行的安全投资效果相当于 $s_2 = s_2 + \lambda_1 s_1$,其中 $\lambda_1 \in [0, 1]$ 和 $\lambda_2 \in [0, 1]$ 分别是企业1与企业2的信息共享系数. 因此黑客对企业1的入侵概率函数为 $\rho_1 = \xi_1 c_1^{k_1(s_1+\lambda_2 s_2)+1}$,对企业2的入侵概率函数为 $\rho_2 = \xi_2 c_2^{k_2(s_2+\lambda_1 s_1)+1}$. 把 ρ_1 和 ρ_2 分别代入企业1和企业2的期望效用函数

$$EU_1 = \rho_1(\beta - \alpha e^{-\alpha(w_1-s_1-L_1)}) + (1 - \rho_1)(\beta - \alpha e^{-\alpha(w_1-s_1)}), \quad (1)$$

$$EU_2 = \rho_2(\beta - \alpha e^{-\alpha(w_2-s_2-L_2)}) + (1 - \rho_2)(\beta - \alpha e^{-\alpha(w_2-s_2)}). \quad (2)$$

对企业1的期望效用关于 s_1 求一阶偏导和二阶偏导,得

$$\frac{\partial EU_1}{\partial s_1} = \alpha e^{-\alpha(w_1-s_1)} \left(\frac{\partial \rho_1}{\partial s_1} (1 - e^{\alpha L_1}) + \alpha \rho_1 (1 - e^{\alpha L_1}) - \alpha \right), \quad (3)$$

$$\frac{\partial^2 EU_1}{\partial s_1^2} = \alpha e^{-\alpha(w_1-s_1)} \left(\xi_1 c_1^{k_1(s_1+\lambda_2 s_2)+1} (1 - e^{\alpha L_1}) (k_1 \ln(c_1) + \alpha)^2 - \alpha^2 \right). \quad (4)$$

当 $\alpha > 0$ 时,易知 $\frac{\partial^2 EU_1}{\partial s_1^2} < 0$,故可知 EU_1 存在最大值.

同理可得

$$\frac{\partial EU_2}{\partial s_2} = \alpha e^{-\alpha(w_2-s_2)} \left(\frac{\partial \rho_2}{\partial s_2} (1 - e^{\alpha L_2}) + \alpha \rho_2 (1 - e^{\alpha L_2}) - \alpha \right), \quad (5)$$

$$\frac{\partial^2 EU_2}{\partial s_2^2} < 0, EU_2 \text{ 存在最大值.}$$

把

$$\begin{aligned} \rho_1 &= \xi_1 c_1^{k_1(s_1+\lambda_2 s_2)+1}, \frac{\partial \rho_1}{\partial s_1} = k_1 \ln(c_1) \xi_1 c_1^{k_1(s_1+\lambda_2 s_2)+1}, \\ \rho_2 &= \xi_2 c_2^{k_2(s_2+\lambda_1 s_1)+1}, \frac{\partial \rho_2}{\partial s_2} = k_2 \ln(c_2) \xi_2 c_2^{k_2(s_2+\lambda_1 s_1)+1}, \end{aligned}$$

代入, 求解 $\frac{\partial EU_1}{\partial s_1} = 0$ 和 $\frac{\partial EU_2}{\partial s_2} = 0$, 可得企业1和企业2的最优投资如下

$$s_1 = \frac{1}{1 - \lambda_1 \lambda_2} \left(\frac{1}{k_1 \ln(c_1)} \ln \frac{\alpha}{\xi_1 c_1 (\ln(c_1) + \alpha) (1 - e^{\alpha L_1})} - \frac{\lambda_2}{k_2 \ln(c_2)} \ln \frac{\alpha}{\xi_2 c_2 (\ln(c_2) + \alpha) (1 - e^{\alpha L_2})} \right), \quad (6)$$

$$s_2 = \frac{1}{1 - \lambda_1 \lambda_2} \left(\frac{1}{k_2 \ln(c_2)} \ln \frac{\alpha}{\xi_2 c_2 (\ln(c_2) + \alpha) (1 - e^{\alpha L_2})} - \frac{\lambda_1}{k_1 \ln(c_1)} \ln \frac{\alpha}{\xi_1 c_1 (\ln(c_1) + \alpha) (1 - e^{\alpha L_1})} \right). \quad (7)$$

当两企业对称, 即当两企业的安全投资效率、网络暴露程度、潜在损失、两企业信息共享率分别相等时 ($k_1 = k_2 = k, c_1 = c_2 = c, \xi_1 = \xi_2 = \xi, L_1 = L_2 = L, \lambda_1 = \lambda_2 = \lambda$)

$$s = \frac{1}{(1 + \lambda)(k \ln(c))} \ln \frac{\alpha}{\xi c (\ln(c) + \alpha) (1 - e^{\alpha L})} = \frac{1}{(1 + \lambda)(k \ln(c))} (\ln \alpha - \ln(\xi c (\ln(c) + \alpha) (1 - e^{\alpha L}))). \quad (8)$$

由于模型考虑的因素比较多, 分析起来有些复杂, 因此以下命题1是对两企业对称情况的讨论.

命题1 随机攻击情形下, 当企业极度厌恶风险时, 企业最优安全投资随着风险厌恶水平的增加而增加; 当企业轻微厌恶风险时, 若潜在损失 L 较大或者黑客攻击概率 ξ 较大或者网络暴露程度 c 中等时, 即 $L > -\frac{2}{\xi c \ln(c)}$ 时, 最优安全投资随着风险厌恶水平的增加而增加, 当潜在损失较小或者黑客攻击概率较小或者网络暴露程度太高或太低时, 即 $0 < L < -\frac{2}{\xi c \ln(c)}$ 时, 企业的最优安全投资随着风险厌恶水平的增加而减小.

证明 对风险厌恶系数进行求偏导

$$\frac{\partial s}{\partial \alpha} = \frac{1}{(1 + \lambda)(k \ln(c))} \left(\frac{(e^{\alpha L} - 1) - \alpha L}{\alpha(e^{\alpha L} - 1)} - \frac{1}{\xi c (\ln(c) + \alpha)} - L \right). \quad (9)$$

当企业极度厌恶风险, 即当 $\alpha \rightarrow +\infty$ 时,

$$\frac{\partial s}{\partial \alpha} \Big|_{\alpha \rightarrow +\infty} = -\frac{1}{(1 + \lambda)(k \ln(c))} L > 0. \quad (10)$$

因此, 企业的最优信息安全投资随着风险厌恶水平的增加而增加. 当企业轻微厌恶风险, 即当 $\alpha \rightarrow 0^+$ 时, 设 $A = \frac{(e^{\alpha L} - 1) - \alpha L}{\alpha(e^{\alpha L} - 1)}$, $A \Big|_{\alpha \rightarrow 0^+} \rightarrow \frac{L}{2}$,

$$\frac{\partial s}{\partial \alpha} \Big|_{\alpha \rightarrow 0^+} \rightarrow -\frac{1}{(1 + \lambda)(k \ln(c))} \left(\frac{1}{\xi c \ln(c)} + \frac{L}{2} \right). \quad (11)$$

由于 $0 < c < 1$, 因此 $\ln(c) < 0$, 当 $\frac{1}{\xi c \ln(c)} + \frac{L}{2} < 0$, 即 $0 < L < -\frac{2}{\xi c \ln(c)}$, $0 < \xi < -\frac{2}{L c \ln(c)}$, $c \ln(c) > -\frac{2}{\xi L}$ 时, $\frac{\partial s}{\partial \alpha} \Big|_{\alpha \rightarrow 0^+} < 0$; 当 $\frac{1}{\xi c \ln(c)} + \frac{L}{2} > 0$, 即 $L > -\frac{2}{\xi c \ln(c)}$, $-\frac{2}{L c \ln(c)} < \xi < 1$, $c \ln(c) < -\frac{2}{L \xi}$ 时, 有 $\frac{\partial s}{\partial \alpha} \Big|_{\alpha \rightarrow 0^+} > 0$. 证毕.

因此, 当企业轻微厌恶风险时, 企业的最优安全投资还需要考虑网络暴露程度、黑客的攻击概率和潜在

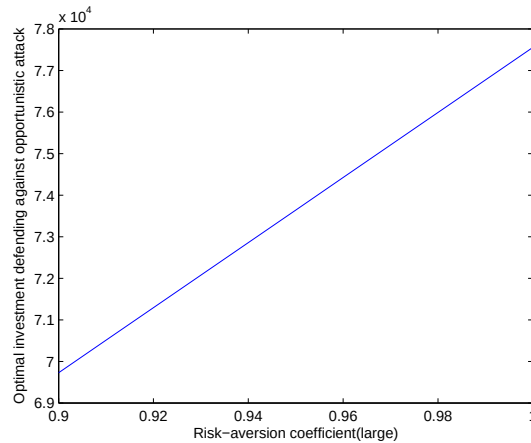


图1 随机攻击下最优安全投资与风险厌恶系数的关系(极度厌恶风险)

Fig.1 Optimal information security investment vs. great high risk-aversion coefficient

损失的大小,若潜在损失较大或者黑客的攻击概率比较大或者网络暴露程度中等时,企业的最优安全投资随着风险厌恶水平的增加而增加,若潜在损失较小或者黑客的攻击概率较小或者网络暴露程度太高或太低时,企业的最优安全投资随着风险厌恶水平的增加而减小。

由以上结论可知,在随机攻击情形下,企业如果非常厌恶风险,当风险增大时,在企业获得最大期望效用的情况下,企业对网络的安全投资总是在增加的。当企业轻微厌恶风险时,最优信息安全投资视情况而定。当潜在损失较大或者黑客的攻击概率较大或者网络暴露程度中等时,企业要想获得最大期望效用就应该增加信息安全投资;当潜在损失较小或者黑客的攻击概率较小或者网络暴露程度太高或者太低时,企业没有必要为了较小的潜在损失或者较小的攻击概率或者较低的网络暴露程度进行过多的安全投资。网络暴露程度太高,黑客可以以各种方式从更多的路径对企业进行攻击,因此也不宜增加信息安全投资,企业要想获得最大期望效用应该减少信息安全投资。

当企业对风险极度厌恶时,令 $k_1 = k_2 = 0.000\ 005$, $\xi_1 = \xi_2 = 0.4$, $L_1 = L_2 = 2\ 000$, $\lambda_1 = \lambda_2 = 0.3$, $c_1 = c_2 = 0.04$,对最优安全投资与风险厌恶水平的关系进行数学模拟如图1所示。令 $k_1 = k_2 = 0.000\ 005$, $\xi_1 = \xi_2 = 0.4$, $L_1 = L_2 = 200\ 000$, $\lambda_1 = \lambda_2 = 0.3$, $c_1 = c_2 = 0.4$,当企业对风险轻微厌恶时,对最优安全投资与风险厌恶水平的关系进行数学模拟,如图2(a)所示,调整网络暴露程度、潜在损失等参数的大小,令 $k_1 = k_2 = 0.000\ 005$, $\xi_1 = \xi_2 = 0.4$, $L_1 = L_2 = 2\ 000\ 000$, $\lambda_1 = \lambda_2 = 0.3$, $c_1 = c_2 = 0.999\ 99$ 对最优安全投资与风险厌恶水平的关系再次进行数学模拟,如图2(b)所示。

命题2 随机攻击情形下,当企业极度厌恶风险时,企业的最优安全投资随着投资效率的增加而减小;当企业轻微厌恶风险时,若潜在损失 L_1 较小或者黑客的攻击概率 ξ_1 较小或者网络暴露程度 c_1 太高或者太低,即 $0 < L_1 < -\frac{1}{\xi_1 c_1 \ln(c_1)}$ 时,最优安全投资随着投资效率的增加而增加,若潜在损失较大或者黑客的攻击概率较大或者网络暴露程度中等时,即 $L_1 > -\frac{1}{\xi_1 c_1 \ln(c_1)}$ 时,企业的最优安全投资则随着投资效率的增加而减小。

证明

$$\frac{\partial s_1}{\partial k_1} = -\frac{1}{k_1^2(1 - \lambda_1 \lambda_2) \ln(c_1)} \ln \frac{\alpha}{\xi_1 c_1 (\ln(c_1) + \alpha)(1 - e^{\alpha L_1})}. \quad (12)$$

设 $A = \ln \frac{\alpha}{\xi_1 c_1 (\ln(c_1) + \alpha)(1 - e^{\alpha L_1})}$, 由于 $\ln(c_1) + \alpha < 0$, $\alpha < -\ln(c_1)$, 当企业极度厌恶风险, 即当 $\alpha \rightarrow +\infty$ 时, 网络暴露程度 $c_1 \rightarrow 0^+$, 此时 $A|_{\alpha \rightarrow +\infty} \rightarrow -\infty$, 有 $\frac{\partial s_1}{\partial k_1}|_{\alpha \rightarrow +\infty} \rightarrow -\infty < 0$, 因此随机攻击情形下, 当企业极度厌恶风险且网络暴露程度极小的情况下, 企业的最优安全投资随着投资效率的增大而减少; 当企

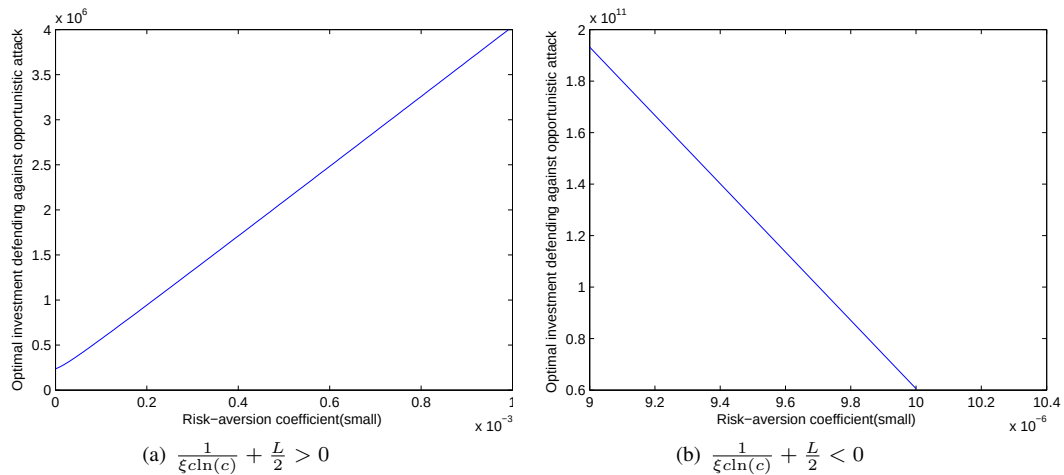


图2 随机攻击下最优信息安全投资与风险厌恶系数的关系(轻微厌恶)

Fig.2 Optimal information security investment vs. very low risk-aversion coefficient

业轻微厌恶风险, 即当 $\alpha \rightarrow 0^+$ 时,

$$\frac{\partial s_1}{\partial k_1} \Big|_{\alpha \rightarrow 0^+} \rightarrow \frac{1}{k_1^2(1 - \lambda_1 \lambda_2) \ln(c_1)} \ln(-\xi_1 c_1 \ln(c_1) L_1). \quad (13)$$

注意到 $0 < c_1 < 1$, $\ln(c_1) < 0$, 当 $\ln(-\xi_1 c_1 \ln(c_1) L_1) < 0$, 即 $0 < L_1 < -\frac{1}{\xi_1 c_1 \ln(c_1)}$, $0 < \xi_1 < -\frac{1}{L_1 c_1 \ln(c_1)}$, $c_1 \ln(c_1) > -\frac{1}{\xi_1 L_1}$ 时, 有 $\frac{\partial s_1}{\partial k_1} \Big|_{\alpha \rightarrow 0^+} > 0$. 证毕.

因此, 若潜在损失较小或者黑客的攻击概率较小或者网络暴露程度太高或太低时, 最优安全投资随着投资效率的增加而增加; 若潜在损失较大或者黑客的攻击概率较大或者网络暴露程度中等时, 最优安全投资随着投资效率的增加而减小.

随机攻击情形下, 企业极度厌恶风险且网络暴露程度极小时, 当安全投资效率提高时, 企业的最优安全投资随着投资效率的增大而减少, 这是因为安全投资效率提高使企业网络系统的安全水平提高, 此时网络暴露程度极小, 一般情况下并不能对企业的网络系统构成威胁, 为了获得最大期望效用, 风险厌恶型决策者不愿意再增加安全投资. 从实践来看, 定向攻击入侵相对随机攻击入侵来说带给企业更大的潜在损失, 当安全投资效率提高时应该增大企业的信息安全投资, 根据本结论可知, 在网络暴露程度极小的情况下可以适当减小信息安全投资. 如果企业轻微厌恶风险, 最优安全投资视情况而定, 在潜在损失较小或者黑客的攻击概率较小或者网络暴露程度太高或者太低的情况下, 当企业安全投资效率增加时, 增加安全投资可以快速提高网络安全水平, 获得最大期望效用, 因此风险厌恶型决策愿意增加安全投资; 若潜在损失较大或者黑客的攻击概率较大或者网络暴露程度满足中等时, 在企业安全投资效率增加时, 企业网络系统的安全水平增高, 企业为了获得最大期望效用将会减少安全投资.

当企业对风险极度厌恶时, 令风险厌恶系数 $\alpha = 20$, 黑客攻击概率 $\xi_1 = \xi_2 = 0.04$, 潜在损失 $L_1 = L_2 = 20$, 信息共享率 $\lambda_1 = 0.6$, $\lambda_2 = 0.3$, 网络暴露程度 $c_1 = c_2 = 0.000\ 001$, 对最优安全投资与安全投资效率的关系进行数学模拟如图3所示. 当企业对风险轻微厌恶时, 令风险厌恶系数 $\alpha = 0.000\ 01$, 黑客攻击概率 $\xi_1 = \xi_2 = 0.4$, 潜在损失 $L_1 = L_2 = 20\ 000$, 信息共享率 $\lambda_1 = 0.6$, $\lambda_2 = 0.3$, 网络暴露程度 $c_1 = c_2 = 0.999\ 9$, 对最优安全投资与安全投资效率的关系进行数学模拟如图4(a)所示. 当企业对风险轻微厌恶时, 风险厌恶系数 $\alpha = 0.000\ 01$ 保持不变, 调整网络暴露程度等参数的大小, 令网络暴露程度 $c_1 = c_2 = 0.04$, 黑客攻击概率 $\xi_1 = \xi_2 = 0.4$, 潜在损失 $L_1 = L_2 = 20\ 000$, 信息共享率 $\lambda_1 = 0.6$, $\lambda_2 = 0.3$, 对最优安全投资与安全投资效率的关系再次进行数学模拟如图4(b)所示.

命题3 随机攻击情形下, 企业1与企业2的最优安全投资随着各自共享系数的增加而增加.

证明

$$\frac{\partial s_1}{\partial \lambda_1} = \frac{\lambda_2}{(1 - \lambda_1 \lambda_2)^2} \left(\frac{1}{k_1 \ln(c_1)} \ln \frac{\alpha}{\xi_1 c_1 (\ln(c_1) + \alpha)(1 - e^{\alpha L_1})} - \frac{\lambda_2}{k_2 \ln(c_2)} \ln \frac{\alpha}{\xi_2 c_2 (\ln(c_2) + \alpha)(1 - e^{\alpha L_2})} \right). \quad (14)$$

为了投资有意义, 需

$$\frac{1}{k_1 \ln(c_1)} \ln \frac{\alpha}{\xi_1 c_1 (\ln(c_1) + \alpha)(1 - e^{\alpha L_1})} - \frac{\lambda_2}{k_2 \ln(c_2)} \ln \frac{\alpha}{\xi_2 c_2 (\ln(c_2) + \alpha)(1 - e^{\alpha L_2})} > 0. \quad (15)$$

很显然 $\frac{\partial s_1}{\partial \lambda_1} > 0$. 当企业增大信息共享率时, 一方面提高了各个企业的安全水平, 同时也增大了各企业的安全投资. 证毕.

令企业2的信息安全共享率 $\lambda_2 = 0.3$, 网络暴露程度 $c_1 = c_2 = 0.4$, 风险厌恶系数 $\alpha = 0.001$, 安全投资效率 $k_1 = k_2 = 0.0005$, 黑客攻击概率 $\xi_1 = \xi_2 = 0.04$, 潜在损失 $L_1 = L_2 = 20\,000$, 对企业最优安全投资与各自信息共享系数的关系进行数学模拟如图5所示.

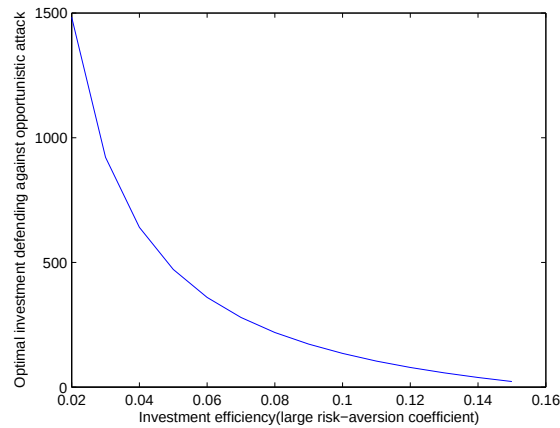
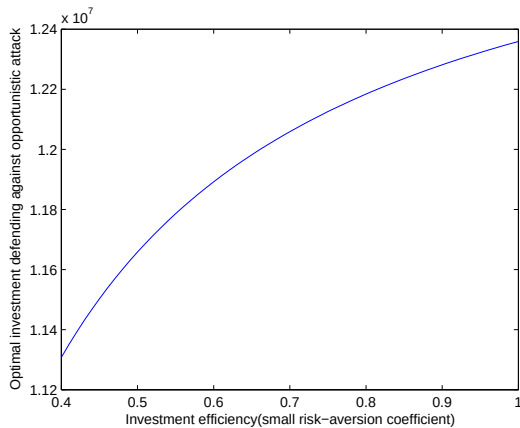
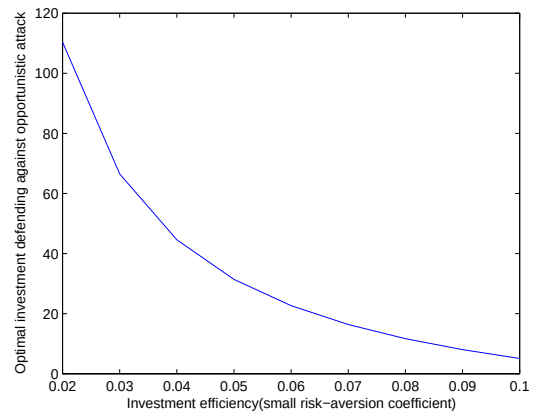


图3 随机攻击下最优安全投资与投资效率的关系(极度厌恶风险)

Fig.3 Optimal information security investment vs.investment efficiency with great high risk-aversion coefficient



(a) $\ln(-\xi_1 c_1 \ln(c_1) L_1) < 0$



(b) $\ln(-\xi_1 c_1 \ln(c_1) L_1) > 0$

图4 随机攻击下最优安全投资与投资效率的关系(轻微厌恶风险)

Fig.4 Optimal information security investment vs.investment efficiency with very low risk-aversion coefficient

2.3 定向攻击情形下的信息安全投资策略

定向攻击情形下, 当两企业进行信息共享时, 企业1和企业2受到黑客的入侵概率分别为 $\rho_1 = \frac{\xi_1 c_1}{k_1(s_1 + \lambda_2 s_2) + 1}$ 和 $\rho_2 = \frac{\xi_2 c_2}{k_2(s_2 + \lambda_1 s_1) + 1}$, $\frac{\partial \rho_1}{\partial s_1} = -\frac{k_1 \xi_1 c_1}{(k_1(s_1 + \lambda_2 s_2) + 1)^2}$, $\frac{\partial \rho_2}{\partial s_2} = -\frac{k_2 \xi_2 c_2}{(k_2(s_2 + \lambda_1 s_1) + 1)^2}$,

并代入企业1的期望效用, 对企业1的期望效用关于 s_1 求一阶偏导和二阶偏导, 得

$$EU_1 = \rho_1(\beta - \alpha e^{-\alpha(w_1 - s_1 - L_1)}) + (1 - \rho_1)(\beta - \alpha e^{-\alpha(w_1 - s_1)}), \quad (16)$$

故

$$\frac{\partial EU_1}{\partial s_1} = \alpha e^{-\alpha(w_1 - s_1)} \left(\frac{\partial \rho_1}{\partial s_1} (1 - e^{\alpha L_1}) + (1 - e^{\alpha L_1}) \alpha \rho_1 - \alpha \right), \quad (17)$$

$$\begin{aligned} \frac{\partial^2 EU_1}{\partial s_1^2} = & \alpha e^{-\alpha(w_1 - s_1)} \left((1 - e^{\alpha L_1}) \frac{\xi_1 c_1}{k_1(s_1 + \lambda_2 s_2) + 1} \left(\left(\frac{k_1}{(k_1(s_1 + \lambda_2 s_2) + 1)} - \alpha \right)^2 + \right. \right. \\ & \left. \left. \frac{k_1^2}{(k_1(s_1 + \lambda_2 s_2) + 1)^2} \right) - \alpha^2 \right). \end{aligned} \quad (18)$$

当 $\alpha > 0$ 时, 易知 $\frac{\partial^2 EU_1}{\partial s_1^2} < 0$, 故可知 EU_1 存在最大值.

同理可得

$$EU_2 = \rho_2(\beta - \alpha e^{-\alpha(w_2 - s_2 - L_2)}) + (1 - \rho_2)(\beta - \alpha e^{-\alpha(w_2 - s_2)}), \quad (19)$$

故

$$\frac{\partial EU_2}{\partial s_2} = \alpha e^{-\alpha(w_2 - s_2)} \left(\frac{\partial \rho_2}{\partial s_2} (1 - e^{\alpha L_2}) + (1 - e^{\alpha L_2}) \alpha \rho_2 - \alpha \right), \quad (20)$$

$$\begin{aligned} \frac{\partial^2 EU_2}{\partial s_2^2} = & \alpha e^{-\alpha(w_2 - s_2)} \left((1 - e^{\alpha L_2}) \frac{\xi_2 c_2}{k_2(s_2 + \lambda_1 s_1) + 1} \left(\left(\frac{k_2}{(k_2(s_2 + \lambda_1 s_1) + 1)} - \alpha \right)^2 + \right. \right. \\ & \left. \left. \frac{k_2^2}{(k_2(s_2 + \lambda_1 s_1) + 1)^2} \right) - \alpha^2 \right). \end{aligned} \quad (21)$$

当 $\alpha > 0$ 时, $\frac{\partial^2 EU_2}{\partial s_2^2} < 0$, EU_2 存在最大值.

设 $\Delta_1 = \alpha^2 + 4k_1 \frac{\alpha}{\xi_1 c_1 (e^{\alpha L_1} - 1)} \geq 0$, $\Delta_2 = \alpha^2 + 4k_2 \frac{\alpha}{\xi_2 c_2 (e^{\alpha L_2} - 1)} \geq 0$, 则企业1与企业2的最优安全投资为

$$s_1 = \frac{1}{(1 - \lambda_1 \lambda_2)} \left(\frac{2}{\alpha + \sqrt{\Delta_1}} - \frac{2\lambda_2}{\alpha + \sqrt{\Delta_2}} + \frac{\lambda_2}{k_2} - \frac{1}{k_1} \right), \quad (22)$$

$$s_2 = \frac{1}{(1 - \lambda_1 \lambda_2)} \left(\frac{2}{\alpha + \sqrt{\Delta_2}} - \frac{2\lambda_1}{\alpha + \sqrt{\Delta_1}} + \frac{\lambda_1}{k_1} - \frac{1}{k_2} \right). \quad (23)$$

当两企业对称时, 两企业的安全投资效率、网络暴露程度、潜在损失、两企业信息共享率分别相等 ($k_1 = k_2 = k, c_1 = c_2 = c, \xi_1 = \xi_2 = \xi, L_1 = L_2 = L, \lambda_1 = \lambda_2 = \lambda$), 以下命题4是对两企业对称情况的讨论.

命题4 定向攻击情形下, 当企业极度厌恶风险时, 最优安全投资随着风险厌恶水平的增加而减小, 当企业轻微厌恶风险时, 若网络暴露程度、黑客攻击概率、潜在损失和安全投资效率满足关系 $\frac{\xi c L e^{\alpha L} (1 - A)}{2k} + \frac{1}{A} \left(\frac{1}{\alpha^2} + \frac{1}{L \alpha (e^{\alpha L} - 1)} \right) < 0$ 时, 最优安全投资随风险厌恶水平的增加而增加, 若满

足关系 $\frac{\xi c L e^{\alpha L}(1-A)}{2k} + \frac{1}{A} \left(\frac{1}{\alpha^2} + \frac{1}{L\alpha(e^{\alpha L}-1)} \right) > 0$ 时, 最优安全投资随着风险厌恶水平的增加而减小。

证明

$$\begin{aligned} s &= \frac{1}{(1+\lambda)} \left(\frac{2}{(\alpha + \sqrt{\Delta_2})} - \frac{1}{k} \right) \\ &= -\frac{1}{(1+\lambda)} \left(\frac{\xi c(e^{\alpha L}-1) \left(1 - \sqrt{1 + 4k \frac{1}{\xi c \alpha(e^{\alpha L}-1)}} \right)}{2k} + \frac{1}{k} \right) \\ &= -\frac{1}{(1+\lambda)} \left(\frac{\xi c(e^{\alpha L}-1) + 2}{2k} - \frac{\xi c(e^{\alpha L}-1) \sqrt{1 + 4k \frac{1}{\xi c \alpha(e^{\alpha L}-1)}}}{2k} \right). \end{aligned} \quad (24)$$

设 $A = \left(1 + \frac{4k}{\xi c \alpha(e^{\alpha L}-1)} \right)^{\frac{1}{2}}$ 则

$$\frac{\partial A}{\partial \alpha} = -\frac{2k}{\xi c \alpha(e^{\alpha L}-1)} \left(1 + \frac{4k}{\xi c \alpha(e^{\alpha L}-1)} \right)^{-\frac{1}{2}} \left(\frac{1}{\alpha} + \frac{1}{L(e^{\alpha L}-1)} \right), \quad (25)$$

$$\frac{\partial s}{\partial \alpha} = -\frac{1}{(1+\lambda)} \left(\frac{\xi c L e^{\alpha L}(1-A)}{2k} + \frac{1}{A} \left(\frac{1}{\alpha^2} + \frac{1}{L\alpha(e^{\alpha L}-1)} \right) \right). \quad (26)$$

企业面对定向攻击情形下, 当企业极度厌恶风险, 即当 $\alpha \rightarrow +\infty$ 时, $A|_{\alpha \rightarrow +\infty} \rightarrow 1^+$, $\frac{\partial s}{\partial \alpha}|_{\alpha \rightarrow +\infty} \rightarrow 0^- < 0$, 因此, 最优信息安全投资随风险厌恶水平的增加而减小. 当企业轻微厌恶风险时, 即当 $\alpha \rightarrow 0^+$ 时, 若 $\frac{\xi c L e^{\alpha L}(1-A)}{2k} + \frac{1}{A} \left(\frac{1}{\alpha^2} + \frac{1}{L\alpha(e^{\alpha L}-1)} \right) < 0$, 则 $\frac{\partial s}{\partial \alpha} > 0$, 若 $\frac{\xi c L e^{\alpha L}(1-A)}{2k} + \frac{1}{A} \left(\frac{1}{\alpha^2} + \frac{1}{L\alpha(e^{\alpha L}-1)} \right) > 0$, $\frac{\partial s}{\partial \alpha} < 0$. 因此, 当企业轻微厌恶风险时, 还需要考虑网络暴露程度、黑客攻击概率、潜在损失、安全投资效率与风险厌恶程度的关系, 若满足关系 $\frac{\xi c L e^{\alpha L}(1-A)}{2k} + \frac{1}{A} \left(\frac{1}{\alpha^2} + \frac{1}{L\alpha(e^{\alpha L}-1)} \right) < 0$, 最优安全投资随着风险厌恶水平的增加而增加, 若满足关系 $\frac{\xi c L e^{\alpha L}(1-A)}{2k} + \frac{1}{A} \left(\frac{1}{\alpha^2} + \frac{1}{L\alpha(e^{\alpha L}-1)} \right) > 0$, 最优安全投资随着风险厌恶水平的增大而减小. 证毕.

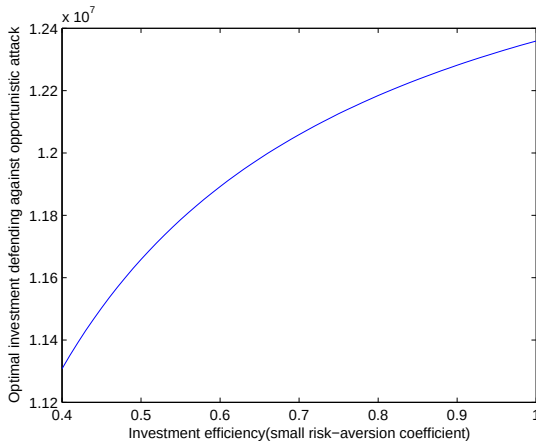


图5 随机攻击下最优安全投资与信息共享系数的关系

Fig.5 Optimal information security investment vs. information sharing coefficient

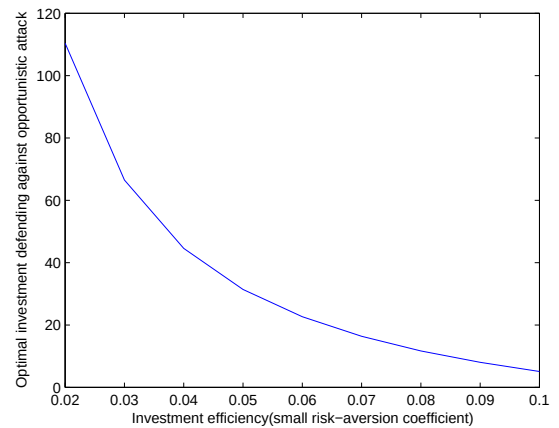


图6 定向攻击下最优安全投资与风险厌恶水平的关系(极度厌恶风险)

Fig.6 Optimal information security investment vs great high risk-aversion coefficient

定向攻击情形下, 当企业极度厌恶风险时, 其最优安全投资随着风险厌恶水平的增加而减小, 这和实践存在一定分歧, 本研究认为, 当企业进行安全投资决策时, 考虑的不仅有安全风险(黑客入侵造成损失的风险), 还有投资风险(过度投资的风险), 决策者在进行安全投资决策时, 需要平衡安全风险与投资风险的关系. 在投资数额较少时, 投资风险较小, 但安全风险较大, 此时, 风险厌恶型决策者为了提高安全水平就会增大投资. 随着投资额的增大, 网络安全水平提高, 安全风险逐渐减小, 但投资风险增大, 此时, 风险厌恶型决策者为降低投资风险, 就会适当减少投资.

当企业对风险极度厌恶时, 令 $k_1 = k_2 = 0.005$, $\xi_1 = \xi_2 = 0.4$, $L_1 = L_2 = 2\ 000$, $\lambda_1 = 0.6$, $\lambda_2 = 0.3$, $c_1 = c_2 = 0.04$, 对最优信息安全投资与风险厌恶水平的关系进行数学模拟如图6所示.

当企业轻微厌恶风险时, 其它参数不变, 改变风险厌恶系数的取值范围, 对最优安全投资与风险厌恶水平的关系进行数学模拟, 如图7(a)所示. 当企业对风险轻微厌恶时, 调整潜在损失 $L_1 = L_2 = 200\ 000$, 网络暴露程度 $\xi_1 = \xi_2 = 0.8$, 安全投资效率 $k_1 = k_2 = 0.04$, 对最优安全投资与风险厌恶水平的关系进行数学模拟, 如图7(b)所示.

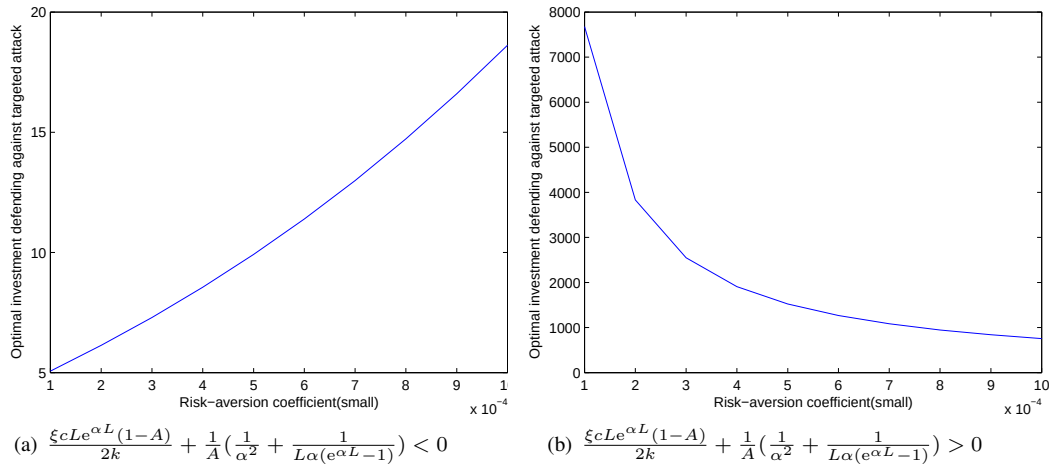


图7 定向攻击下最优安全投资与风险厌恶水平的关系(轻微厌恶风险)

Fig.7 Optimal information security investment vs. very low risk-aversion coefficient

命题5 定向攻击情形下, 企业的最优安全投资随着安全投资效率的增加而增加, 与企业对风险的厌恶水平无关.

证明

$$\frac{\partial s_1}{\partial k_1} = \frac{1}{(1 - \lambda_1 \lambda_2)} \left(\frac{2\xi_1 c_1 (e^{\alpha L_1} - 1)}{4k_1^2} + \frac{1}{\sqrt{(\alpha^2 + 4k_1 \frac{\alpha}{\xi_1 c_1 (e^{\alpha L_1} - 1)})}} + \frac{2\xi_1 c_1 (1 - e^{\alpha L_1}) \sqrt{\alpha^2 + 4k_2 \frac{\alpha}{\xi_2 c_2 (e^{\alpha L_2} - 1)}}}{4\alpha k_1^2} + \frac{1}{k_1^2} \right), \quad (27)$$

$$\frac{\partial s_1}{\partial k_1} \Big|_{\alpha \rightarrow 0^+} \rightarrow \frac{1}{(1 - \lambda_1 \lambda_2)} \left(\sqrt{\frac{\xi_1 c_1 L_1}{4k_1}} + \frac{1}{k_1^2} \right) > 0, \quad (28)$$

$$\frac{\partial s_1}{\partial k_1} \Big|_{\alpha \rightarrow +\infty} \rightarrow \frac{1}{k_1^2 (1 - \lambda_1 \lambda_2)} > 0. \quad (29)$$

同理可证 $\frac{\partial s_2}{\partial k_2} \big|_{\alpha \rightarrow +\infty} > 0$, $\frac{\partial s_2}{\partial k_2} \big|_{\alpha \rightarrow 0^+} > 0$.

证毕.

定向攻击情形下, 企业的最优信息安全投资随着安全投资效率的增加而增加, 不受其它因素的影响, 如图8所示. 信息安全投资效率的增高可以有效提高安全水平, 减小定向攻击入侵带来的潜在损失, 风险厌恶型决策者很愿意增大安全投资以减少定向攻击所带来的潜在损失. 由此命题可知, 在企业面临定向攻击时, 当投资效率增大时, 厌恶型决策者应该增加安全投资, 以获得最大期望效用.

厌恶系数 $\alpha = 7$, 黑客攻击概率 $\xi_1 = \xi_2 = 0.4$, 另一个企业的安全投资效率为 $k_2 = 0.05$, 潜在损失 $L_1 = L_2 = 200\,000$, 信息共享率 $\lambda_1 = 0.6$, $\lambda_2 = 0.3$, 网络暴露程度 $c_1 = c_2 = 0.04$, 对定向攻击下最优安全投资与安全投资效率的关系进行数学模拟, 如图8所示.

命题6 定向攻击情形下, 企业1和企业2的最优安全投资都随着本企业信息共享系数的增加而增加.

证明 设 $\Delta_1 = \alpha^2 - 4k_1 \frac{\alpha}{\xi_1 c_1 (1 - e^{\alpha L_1})} \geq 0$, $\Delta_2 = \alpha^2 - 4k_2 \frac{\alpha}{\xi_2 c_2 (1 - e^{\alpha L_2})} \geq 0$, 则

$$s_1 = \frac{1}{(1 - \lambda_1 \lambda_2)} \left(\frac{2}{\alpha + \sqrt{\Delta_1}} - \frac{2\lambda_2}{\alpha + \sqrt{\Delta_2}} + \frac{\lambda_2}{k_2} - \frac{1}{k_1} \right), \quad (30)$$

$$s_2 = \frac{1}{(1 - \lambda_1 \lambda_2)} \left(\frac{2}{\alpha + \sqrt{\Delta_2}} - \frac{2\lambda_1}{\alpha + \sqrt{\Delta_1}} + \frac{\lambda_1}{k_1} - \frac{1}{k_2} \right), \quad (31)$$

$$\frac{\partial s_1}{\partial \lambda_1} = \frac{\lambda_2}{(1 - \lambda_1 \lambda_2)^2} \left(\frac{2}{\alpha + \sqrt{\Delta_1}} - \frac{2\lambda_2}{\alpha + \sqrt{\Delta_2}} + \frac{\lambda_2}{k_2} - \frac{1}{k_1} \right) \geq 0, \quad (32)$$

$$\frac{\partial s_2}{\partial \lambda_2} = \frac{\lambda_1}{(1 - \lambda_1 \lambda_2)^2} \left(\frac{2}{\alpha + \sqrt{\Delta_2}} - \frac{2\lambda_1}{\alpha + \sqrt{\Delta_1}} + \frac{\lambda_1}{k_1} - \frac{1}{k_2} \right) \geq 0. \quad (33)$$

证毕.

从上述计算可以看出, 定向攻击情形下, 企业1和企业2的最优安全投资都随着各自信息共享系数的增加而增加, 如图9所示, 当企业增大信息共享率时, 一方面提高了各个企业的安全水平, 同时也增大了各企业的安全投资, 这一结论与随机攻击情形下的结论相同.

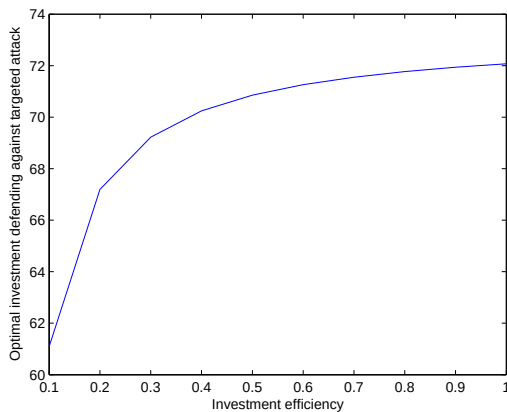


图8 定向攻击下最优安全投资与投资效率的关系

Fig. 8 Optimal information security investment vs. investment efficiency

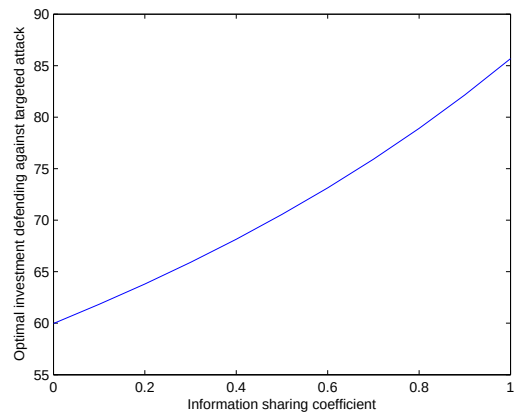


图9 定向攻击下最优安全投资与信息共享系数的关系

Fig. 9 Optimal information security investment vs. information sharing coefficient

任意设置风险厌恶系数 $\alpha = 7$, 令另一个企业的信息安全共享率 $\lambda_2 = 0.3$, 网络暴露程度 $c_1 = c_2 = 0.04$, 安全投资效率 $k_1 = k_2 = 0.000\,005$, 黑客攻击概率 $\xi_1 = \xi_2 = 0.4$, 潜在损失 $L_1 = L_2 = 2\,000\,000$, 对企业最

优安全投资与各自共享系数的关系进行模拟,如图9所示。

通过对随机攻击与定向攻击两种情形下的结论比较可知,除了最优安全投资与信息共享系数的关系相同,其他结论都存在差异。由此可知,当企业同时面临随机攻击与定向攻击时,可参考对应的研究结论并结合企业的具体情况,根据网络暴露程度、黑客攻击概率和潜在损失的关系分别对随机攻击与定向攻击情形下的安全投资做出合理的资金分配,选择最优安全投资以获得最大期望效用。

3 结束语

本文分别对随机攻击与定向攻击两种情形下两个风险厌恶型企业的信息安全投资策略进行了研究,同时考虑了两企业的信息共享水平,并分析了两种攻击情形下风险厌恶水平、企业的潜在损失、网络暴露程度、黑客攻击概率、安全投资效率等相关因素对企业最优安全投资的影响。结果表明,在两种不同的攻击情形下,不同的风险厌恶水平对企业最优信息安全投资具有不同的影响。例如,在随机攻击情形下,当企业极度厌恶风险时,企业的最优信息安全投资随着风险厌恶水平的增加而增加,而定向攻击情形下,当企业极度厌恶风险时,最优安全投资随着风险厌恶水平的增加而减小。

通过对比分析随机攻击与定向攻击两种情形下的结论可以看出,企业面对不同的攻击类型应采取不同的投资策略,才能有效防御黑客的攻击和减少黑客入侵给企业造成的损失。

参考文献:

- [1] Gordon L A, Loeb M P, Zhou L. Investing in cybersecurity: Insights from the gordon-loeb model. *Journal of Information Security*, 2016, 7(2): 49–59.
- [2] Gordon L A, Loeb M P, Lucyshyn W, et al. Increasing cybersecurity investments in private sector firms. *Journal of Information Security*, 2015, 1(1): 3–17.
- [3] Nagurney A, Nagurney L S, Shukla S. A supply chain game theory framework for cybersecurity investments under network vulnerability//*Computation, Cryptography, and Network Security*. Springer, Cham, 2015: 381–398.
- [4] Nagurney A, Daniele P, Shukla S. A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints. *Annals of Operations Research*, 2017, 248(1/2): 405–427.
- [5] Nagurney A, Shukla S. Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. *European Journal of Operational Research*, 2017, 260(2): 588–600.
- [6] 熊 强, 仲伟俊, 梅姝娥. 基于Stackelberg博弈的供应链企业间信息安全决策分析. *情报杂志*, 2012(31): 178–182.
Xiong Q, Zhong W J, Mei S E. Analysis of information security investment decision between supply chain enterprises using stackelberg game. *Journal of Intelligence*, 2012(31): 178–182. (in Chinese)
- [7] Gordon L A, Loeb M P, Lucyshyn W. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, 2003, 22(6): 461–485.
- [8] Gordon L A, Loeb M P, Lucyshyn W, et al. The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*, 2015, 34(5): 509–519.
- [9] Gao X, Zhong W, Mei S. A game-theoretic analysis of information sharing and security investment for complementary firms. *Journal of the Operational Research Society*, 2014, 65(11): 1682–1691.
- [10] Gao X, Zhong W, Mei S. Security investment and information sharing under an alternative security breach probability function. *Information Systems Frontiers*, 2015, 17(2): 423–438.
- [11] Cavusoglu H, Raghunathan S, Yue W T. Decision-theoretic and game-theoretic approaches to IT security investment. *Journal of Management Information Systems*, 2008, 25(2): 281–304.
- [12] Gal-Or E, Ghose A. The economic incentives for sharing security information. *Information Systems Research*, 2005, 16(2): 186–208.
- [13] Schechter S, Smith M. How much security is enough to stop a thief?//*International Conference on Financial Cryptography*. Berlin: Springer, 2003: 122–137.

- [14] 杨丰梅, 王安瑛, 吴 军, 等. 电商平台信用信息共享策略演化. 系统工程学报, 2017, 32(5): 596–603.
Yang F M, Wang A Y, Wu J, et al. Evolutionary dynamics of E-commerce platform's credit information sharing strategy. *Journal of Systems Engineering*, 2017, 32(5): 596–603. (in Chinese)
- [15] 张子辰, 雒兴刚. 考虑广告效应和信息共享的双渠道供应链分析. 系统工程学报, 2017, 32(4): 499–512.
Zhang Z C, Luo X G. Analysis of a dual-channel supply chain with advertising effect and information sharing. *Journal of Systems Engineering*, 2017, 32(4): 499–512. (in Chinese)
- [16] Gao X, Zhong W. Information security investment for competitive firms with hacker behavior and security requirements. *Annals of Operations Research*, 2015, 235(1): 277–300.
- [17] Huang C D, Behara R S. Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. *International Journal of Production Economics*, 2013, 141(1): 255–268.
- [18] Gordon L A, Loeb M P. The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, 2002, 5(4): 438–457.
- [19] Huang C D, Hu Q, Behara R S. An economic analysis of the optimal information security investment in the case of a risk-averse firm. *International Journal of Production Economics*, 2008, 114(2): 793–804.
- [20] 赵柳榕, 梅姝娥, 仲伟俊. 基于风险偏好的两种信息安全技术配置策略. 系统工程学报, 2014, 29(3): 324–333.
Zhao L R, Mei S E, Zhong W J. Configuration strategy of two information security technologies based on risk preference. *Journal of Systems Engineering*, 2014, 29(3): 324–333. (in Chinese)
- [21] 方 玲, 仲伟俊, 梅姝娥. 基于风险偏好的信息系统安全技术策略研究. 科研管理, 2017, 38(12): 166–173.
Fang L, Zhong W J, Mei S E. A research on the information system security technology strategy based on risk preference. *Science Research Management*, 2017, 38(12): 166–173. (in Chinese)
- [22] Friedman M, Savage L J. The expected-utility hypothesis and the measurability of utility. *Journal of Political Economy*, 1952, 60(6): 463–474.
- [23] 徐南荣, 仲伟俊. 现代决策理论与方法. 南京: 东南大学出版社, 2001.
Xu N R, Zhong W J. *Modern Decision Theory and Method*. Ningjing: Southeast University Press, 2001. (in Chinese)
- [24] Wang N. Optimal investment for an insurer with exponential utility preference. *Insurance: Mathematics and Economics*, 2007, 40(1): 77–84.
- [25] Menoncin F. Optimal portfolio and background risk: An exact and an approximated solution. *Insurance: Mathematics and Economics*, 2002, 31(2): 249–265.
- [26] Pratt J W. Risk aversion in the small and in the large. *Econometrica: Journal of the Econometric Society*, 1964, 32(1/2): 122–136.

作者简介:

潘崇霞 (1977—), 女, 山东单县人, 博士生, 研究方向: 信息安全经济学, Email: panchongxia@163.com;

仲伟俊 (1962—), 男, 江苏海安人, 博士, 教授, 研究方向: 信息系统与管理, 电子商务等, Email: zhongweijun@seu.edu.cn;

梅姝娥 (1968—), 女, 江苏南通人, 博士, 教授, 研究方向: 技术创新, 电子商务等, Email: meishue@seu.edu.cn.