·应急管理·

一定预算约束下面对系统不同脆弱性的企业网络安全投资策略研究

□潘崇霞　仲伟俊　梅姝娥
[东南大学　南京　211189]

[摘　要]　针对网络系统不同的脆弱性，通过建模分析了网络暴露程度、黑客攻击概率、黑客入侵概率、安全投资效率等因素对企业的网络安全投资策略的影响，研究了一定预算约束下的企业网络安全投资策略。研究表明：在企业网络系统防御随机攻击能力较强，防御定向攻击能力较弱的情况下，当安全投资总额非常大的时候，对随机攻击类型的投资分配应随着安全投资总额的增大而增大，对定向攻击类型的投资分配应随着安全投资总额的增大而减小；当安全投资总额非常小时，投资分配情况视网络暴露程度的大小而定。

[关键词]　信息安全经济学；网络安全投资；预算约束；随机攻击；定向攻击；网络脆弱性
[中图分类号] F224；TP309　　[文献标识码] A　　[DOI] 10.14071/j.1008-8105(2017)-1013

Enterprise Network Security Investment Strategies When Facing Different Vulnerabilities With Budget Constraints

PAN Chong-xia　ZHONG Wei-jun　MEI Shu-e
(Southeast University　Nanjing　211189　China)

Abstract　This paper develops a model to study enterprise network security investment strategies when facing different vulnerabilities with budget constraints. It analyzes the impact factors such as the network exposure, the attack probability, the breach probability, and security investment efficiency on network security investment strategies. The result shows that under the circumstance that the network system has a stronger ability to defend against an opportunistic attack and a weaker ability to defend against a targeted attack, when the optimal security investment is very high, the investment allocation to the opportunistic attacks increases with an increase in the total investment while investment allocation to the targeted attacks decreases with an increase in the total investment; when the optimal security investment is very small, the allocation of investment depends on the degree of network exposure.

Key words　economics of information security; network security investment; budget constraints; opportunistic attack; targeted attack; network vulnerability

引言

目前，网络安全投资策略研究受到国内外学者的广泛关注，企业网络安全投资策略不仅需要考虑企业信息系统的特点、信息资产的特点、企业的成本、潜在损失，还需要考虑黑客的行为，黑客的攻击类型，黑客的入侵概率、入侵收益、攻击成本等。

[收稿日期]　2017－03－09
[基金项目]　国家自然科学基金项目（71371050）.
[作者简介]　潘崇霞（1977－）女，东南大学经济管理学院博士生；仲伟俊（1962－）男，东南大学经济管理学院教授、博士生导师；梅姝娥（1968－）女，东南大学经济管理学院教授、博士生导师.

黑客的攻击类型一般分为两种：随机攻击（opportunistic attack或mass attack）和定向攻击（targeted attack）。Ponemon机构和Richardson电脑安全机械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、监控软件、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、定向入侵等。

有关黑客攻击方式及其技术的研究，Gao X，Zhong W讨论了两个竞争企业与一个黑客在随机攻击与定向攻击两种攻击情形下的安全投资策略，结果发现，一定条件下，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。论文进一步检验了安全要求对安全投资策略的影响，指出当两企业的竞争比较激烈时，在定向攻击与随机攻击两种情形下，两企业都愿意接受严格的安全管理要求；当两企业的竞争比较温和时，在定向攻击与随机攻击两情形下，两企业都愿意接受宽松的安全管理要求[1]。Xing Gao，Weijun Zhong，Shue Mei采用博弈论方法研究了相关联企业的安全投资，分别考虑了随机攻击、定向攻击和信息系统的薄弱水平，指出并不是所有的安全风险都值得防御，企业面对定向攻击时，应该提高安全投资去弥补信息系统的脆弱水平，而面对随机攻击时，企业应该提高具有中等脆弱水平的信息系统[2]。Png I P L，Wang Q H考虑了随机攻击与定向攻击背景下的两种策略效果的对比：对用户预警和用法律约束攻击者这两种策略哪一种更有效果，结论为，无论是在随机攻击还是在定向攻击的情况下，用户预警都可以减少终端用户的期望损失；当预警成本与攻击成本很低的时候，对用户预警比使用法律约束攻击者更有效；在定向攻击下，在信息安全高估值的情况下，对用户预警更有效，在信息安全较低估值的情况下，法律更有效[3]。

有关信息系统和信息资产脆弱性的研究，Gordon L A，Loeb M P提出了一个在给定信息设置的情况下可以确定最优投资额的经济模型，模型考虑了信息的脆弱性及入侵造成的潜在损失，指出没有必要把投资放到脆弱程度最高的信息资产上面，而应该把投资放到脆弱程度中等的信息资产上面[4]。Y Miaoui，N Boudriga介绍了近年来与企业信息系统及信息资产相关的各种脆弱性研究，并对17年来国家脆弱性数据库数据进行回归分析预测安全投资过程中脆弱程度的演化。结果表明，面对定向攻击的情况下，最优安全投资额总是随着脆弱程度的增大而增大，脆弱类型不同增大程度不同。与定向攻击不同，在随机攻击情形下，最优安全投资额并不总是随着脆弱程度的增大而增大。最优安全投资额还取决于决策者对风险的态度[5]。熊强，仲伟俊，梅姝娥分析了供应链中处于主从地位的两种企业的信息资产价值、网络脆弱性、共享成本、信息安全互补性等因素在供应链信息系统安全决策中的影响，通过建立并比较主从对策模型与Cournot模型两种决策模型，为供应链中各方企业进行信息安全投资及共享决策提供了决策判断依据[6]。Huseyin Cavusoglu，Srinivasan Raghunathan，WeiT Yue采用了博弈论方法来确定信息安全投资水平，并且在安全投资水平、信息系统脆弱性、投资收益方面与决策理论方法进行了比较，研究认为采用博弈方法在一定条件下比采用决策理论更有可能取得最大收益[7]。Nagurney A，Shukla S提出了三个安全投资模型，在合作或竞争的条件下对三个模型进行了均衡分析，并对三个模型中的网络脆弱性与潜在损失的关系进行了比较[8]。Nagurney A，Nagurney L S，Shukla S建立了供应链中多个零售商与多个消费者的期望效用/期望利润的博弈模型，研究了网络脆弱性对安全投资及价格需求函数的影响[9]。Schechter S，Smith M采用经济威胁模型研究了一个企图利用网络脆弱性进入企业系统的对手的行为，而信息共享可以阻止对手入侵，间接提高安全技术的效率[10]。Bandyopadhyay T，Liu D，Mookerjee V S等采用微分博弈模型对两个企业连续时间内的安全投资与一个黑客进行博弈研究，黑客可以根据自己的偏好识别保护能力比较弱的目标，从而造成两个企业之间的竞争，最后推导出稳定均衡解，文献把黑客的偏好定义成两种形式，一种偏好从网络系统的脆弱程度即网络系统入侵的难易程度来选择攻击目标，另一种偏好从信息资产价值选择攻击目标[11]。

企业的投资成本是有限的，需要在一定的资金预算下进行网络安全投资。Huang C D, Behara R S研究了一定预算约束下企业面对多种攻击类型下的信息安全投资，重点研究了企业同时面对随机攻击和定向攻击两种攻击情形下的安全投资，讨论了企业在这两种攻击情形下的最优安全投资及其投资分配[2]。

随着企业安全意识的提高和防病毒软件以及信息系统技术的进步，黑客不再采用单一的攻击方式，一般情况下同时采用不同的攻击方法，即随机攻击和定向攻击相结合的攻击方式。而企业网络系

统由于其自身的特点和投资的侧重点不同存在不同的脆弱性。一些企业自恃信息系统安全等级较高，安全意识淡薄，即使随机攻击中的普通蠕虫病毒也可能使系统遭到入侵。一些企业信息系统安全等级并不高，但平时注意信息系统的更新、安全人员的培训等，即使黑客的定向攻击也能及早发现及时阻止。因此，每个企业的网络系统由于其人员、管理、技术、安全培训等原因具有不同的脆弱性。面对黑客随机攻击与定向攻击相结合的复杂攻击，企业的信息系统由于其脆弱性一般存在两种情形：一种是信息系统防御随机攻击能力较强，防御定向攻击能力较弱，即企业网络系统容易阻止随机攻击的入侵，但不能阻止定向攻击的入侵；另一种是信息系统防御定向攻击能力较强，防御随机攻击能力较弱，即企业网络系统容易阻止定向攻击的入侵，但没能阻止随机攻击的入侵。

论文在参考以前文献的基础上，同时考虑了以上企业信息系统的不同脆弱性和企业的资金预算约束，通过建立经济模型给出了不同脆弱性的网络系统的安全投资及其投资分配策略。

一、模型

攻击类型不同对企业安全投资的影响不同，入侵函数也不同。Gordon，Loeb首先对攻击者的这两种入侵函数进行了区分，称为第一种入侵函数与第二种入侵函数[4]。Huang采用经济学模型研究了一定预算下单个企业在同时面对多种攻击类型时的信息安全投资及其投资分配，文献重点分析了随机攻击和定向攻击两种攻击类型，并从函数上进行了明确区分[7]。对随机攻击入侵函数的定义为：$\rho_1 = \xi_1 c^{k_1 S_1 + 1}$，对定向攻击入侵函数的定义为：$\rho_2 = \dfrac{\xi_2 c}{k_2 S_2 + 1}$，其中参数$c(c \in [0,1])$反应了信息系统的暴露程度，与企业和其他企业的联系频繁程度和网络系统的信息技术有关；$\xi_i (i = 1,2, \xi_i \in [0,1])$表示$i$类型攻击的入侵概率，$S_i (i = 1,2, S_i \geqslant 0)$表示企业面对$i$类型攻击的安全投资，$k_i$，$i = 1,2$，$k_i \in [0,1]$，表示企业面对$i$类型攻击的安全投资效率，$L$表示企业信息系统受到入侵以后的损失。

（一）企业信息系统防御随机攻击能力较强，防御定向攻击能力较弱

企业信息系统防御随机攻击能力较强，防御定向攻击能力较弱，在此情形下意味着企业网络系统容易阻止随机攻击的入侵，却不能阻止定向攻击的入侵。此时黑客对企业信息系统的入侵概率为：$\rho = (1-\rho_1)\rho_2 = (1 - \xi_1 c^{k_1 S_1 + 1}) \dfrac{\xi_2 c}{k_2 S_2 + 1}$。等式右边表示，黑客采取的组合攻击中，随机攻击入侵方式没能成功，但定向攻击成功入侵了企业信息系统。此时企业进行安全投资的期望成本为：

$$\phi(S_1, S_2) = \rho L + (S_1 + S_2) = (1-\rho_1)\rho_2 L + (S_1 + S_2) = (1 - \xi_1 c^{k_1 S_1 + 1}) \frac{\xi_2 c}{k_2 S_2 + 1} L + (S_1 + S_2) \tag{1}$$

由于企业对信息安全的预算投资有限，令$S = S_1 + S_2$，其中S是个常数，把$S_1 = S - S_2$代入（1）得$\phi(S_2) = (1 - \xi_1 c^{k_1 (S - S_2) + 1}) \dfrac{\xi_2 c}{k_2 S_2 + 1} L + S$

结论1：当信息系统防御随机攻击能力较强，防御定向攻击能力较弱时，在暴露程度$c \in (e^{(-k_2/k_1)}, 1]$时，安全投资总额存在最小值$S_0 = \dfrac{1}{(k_1 \ln c)} \ln(\dfrac{k_2}{\xi_1 c (k_1 (\ln c) + k_2)})$；在暴露程度$c \in (0, e^{(-k_2/k_1)})$时，安全投资总额存在最大值$S_0 = \dfrac{1}{(k_1 \ln c)} \ln(\dfrac{k_2}{\xi_1 c (k_1 (\ln c) + k_2)})$。

结论1说明，当暴露程度比较大的时候，企业必须进行一定的投资，投资总额存在最小值；当暴露程度比较小的时候，企业可以进行较少的安全投资，投资总额存在一个最大值。

对结论1的证明如下：

$$\frac{\partial \phi(S_2)}{\partial S_2} = k_1 \xi_1 c^{k_1 (S - S_2) + 1} (\ln c) \frac{\xi_2 c}{k_2 S_2 + 1} L - (1 - \xi_1 c^{k_1 (S - S_2) + 1}) \frac{k_2 \xi_2 c}{(k_2 S_2 + 1)^2} L$$

$$\frac{\partial \phi^2(S_2)}{\partial S_2^2} = -k_1^2 \xi_1 c^{k_1 (S - S_2) + 1} (lnc)^2 \frac{\xi_2 c}{k_2 S_2 + 1} L - 2 k_1 \xi_1 c^{k_1 (S - S_2) + 1} (\ln c) \frac{k_2 \xi_2 c}{(k_2 S_2 + 1)^2} L$$

$$-(1 - \xi_1 c^{k_1 (S - S_2) + 1}) \frac{-2 k_2^2 \xi_2 c}{(k_2 S_2 + 1)^3} L$$

由于企业的安全投资必须有正的收益，使企业的投资边际利润不能为0，否则企业就不会进行投资。所以，当$S_2 = 0$时，需要$\dfrac{\partial \phi(S_2)}{\partial S_2} \geqslant 0$，即

$$k_1 \xi_1 c^{k_1 S + 1} (\ln c) - (1 - \xi_1 c^{k_1 S + 1}) k_2 \geqslant 0,$$

$\xi_1 c^{k_1 S + 1} (k_1 (\ln c) + k_2) \geqslant k_2$，因为$0 < c \leqslant 1$，$lnc \leqslant 0$，当$k_1 (\ln c) + k_2 > 0$，$c > e^{(-k_2/k_1)}$时，

$S \geqslant \frac{1}{(k_1 \ln c)} \ln(\frac{k_2}{\xi_1 c(k_1(\ln c)+k_2)})$；
当$k_1(\ln c)+k_2<0, c<e^{(-k_2/k_1)}$时，
$S \leqslant \frac{1}{(k_1 \ln c)} ln(\frac{k_2}{\xi_1 c(k_1(\ln c)+k_2)})$。

当暴露程度$c \in (e^{(-k_2/k_1)}, 1]$时，假设$c \to 1$，则$\ln c \to 0$，$\frac{\partial \phi^2(S_2)}{\partial S_2^2} \to -(1-\xi_1 c^{k_1(S-S_2)+1}) \frac{-2k_2^2 \xi_2 c}{(k_2 S_2+1)^3} L > 0$；当暴露程度$c \in (0, e^{(-k_2/k_1)})$时，假设$c \to 0$，则$\ln c \to -\infty$，$\frac{\partial \phi^2(S_2)}{\partial S_2^2} \to -\infty < 0$。

因此，在组合攻击下，当暴露程度$c \in (e^{(-k_2/k_1)}, 1]$时，安全投资总额存在最小值$S_0 = \frac{1}{(k_1 \ln c)} \ln(\frac{k_2}{\xi_1 c(k_1(\ln c)+k_2)})$；当暴露程度$c \in (0, e^{(-k_2/k_1)})$时，安全投资总额存在最大值$S_0 = \frac{1}{(k_1 \ln c)} \ln(\frac{k_2}{\xi_1 c(k_1(\ln c)+k_2)})$。

结论2：当信息系统防御随机攻击能力较强，防御定向攻击能力较弱时，在安全投资总额S非常大的时候，对定向攻击类型的投资分配S_2^*/S应随着安全投资总额S的增大而减小，相对应地，对随机攻击类型的投资分配S_1^*/S应随着安全投资总额S的增大而增大。

结论3：当信息系统防御随机攻击能力较强，防御定向攻击能力较弱时，在安全投资总额S非常小时，对定向攻击类型的投资分配S_2^*/S存在两种情况，当信息系统的暴露程度比较小时，对定向攻击类型的投资分配S_2^*/S和对随机攻击类型的投资分配S_1^*/S趋向于一个确定的值，不受安全投资总额S的增大或减小的影响；当信息系统的暴露程度比较大时，对定向攻击类型的投资分配S_2^*/S应随着安全投资总额S的增大而减小，相对应地，对随机攻击类型的投资分配S_1^*/S应随着安全投资总额S的增大而增大。

结论2和结论3证明如下：

令$\frac{\partial \phi(S_2)}{\partial S_2} = F$，即$F = k_1 \xi_1 c^{k_1(S-S_2)+1}(\ln c) \frac{\xi_2 c}{k_2 S_2+1} L - (1-\xi_1 c^{k_1(S-S_2)+1}) \frac{k_2 \xi_2 c}{(k_2 S_2+1)^2} L$

$$\frac{\partial F}{\partial S_2^*} = -k_1^2 \xi_1 c^{k_1(S-S_2)+1}(\ln c)^2 \frac{\xi_2 c}{k_2 S_2+1} L - 2k_1 \xi_1 c^{k_1(S-S_2)+1}(\ln c) \frac{k_2 \xi_2 c}{(k_2 S_2+1)^2} L$$
$$-(1-\xi_1 c^{k_1(S-S_2)+1}) \frac{-2k_2^2 \xi_2 c}{(k_2 S_2+1)^3} L$$

$$\frac{\partial F}{\partial S} = k_1^2 \xi_1 c^{k_1(S-S_2)+1}(\ln c)^2 \frac{\xi_2 c}{k_2 S_2+1} L + k_1 \xi_1 c^{k_1(S-S_2)+1}(\ln c) \frac{k_2 \xi_2 c}{(k_2 S_2+1)^2} L$$

$$\frac{\partial S_2^*/\partial S}{\partial S} = \frac{\partial S_2^*/\partial S}{S} - \frac{S_2^*}{S^2} = \frac{1}{S^2}(-\frac{\partial F/\partial S}{\partial F/\partial S_2^*} - S_2^*)$$

$$= \frac{1}{S^2}(\frac{k_1^2 \xi_1 c^{k_1(S-S_2)+1}(\ln c)^2 \frac{\xi_2 c}{k_2 S_2+1} L + k_1 \xi_1 c^{k_1(S-S_2)+1}(\ln c) \frac{k_2 \xi_2 c}{(k_2 S_2+1)^2} L}{k_1^2 \xi_1 c^{k_1(S-S_2)+1}(\ln c)^2 \frac{\xi_2 c}{k_2 S_2+1} L + 2k_1 \xi_1 c^{k_1(S-S_2)+1}(\ln c) \frac{k_2 \xi_2 c}{(k_2 S_2+1)^2} L} - S_2^*)$$
$$+(1-\xi_1 c^{k_1(S-S_2)+1}) \frac{-2k_2^2 \xi_2 c}{(k_2 S_2+1)^3} L$$

$$= \frac{1}{S^2}(\frac{k_1^2 \xi_1 c^{k_1(S-S_2)+1}(\ln c)^2 + k_1 \xi_1 c^{k_1(S-S_2)+1}(\ln c) \frac{k_2}{k_2 S_2+1}}{k_1^2 \xi_1 c^{k_1(S-S_2)+1}(\ln c)^2 + 2k_1 \xi_1 c^{k_1(S-S_2)+1}(\ln c) \frac{k_2}{k_2 S_2+1}} - S_2^*)$$
$$+(1-\xi_1 c^{k_1(S-S_2)+1}) \frac{-2k_2^2}{(k_2 S_2+1)^2}$$

$$\frac{1}{S^2}(\frac{k_1^2 \xi_1 c(\ln c)^2 + k_1 \xi_1 c(\ln c) k_2}{k_1^2 \xi_1 c(\ln c)^2 + 2k_1 \xi_1 c(\ln c) k_2 + (1-\xi_1 c) - 2k_2^2})$$

当$S \to \infty$时，$c^{k_1(S-S_2^*)} \to 0$，$\frac{\partial S_2^*/\partial S}{\partial S} \to -\frac{S_2^*}{S^2} \leq 0$；当$S \to 0$时，$S_2^* \to 0$，$c^{k_1(S-S_2^*)} \to 1$，$\frac{\partial S_2^*/\partial S}{\partial S} \to \frac{1}{S^2}$

$$\left(\frac{k_1^2\xi_1 c(\ln c)^2+k_1\xi_1 c(\ln c)k_2}{k_1^2\xi_1 c(\ln c)^2+2k_1\xi_1 c(\ln c)k_2+1-\xi_1 c-2k_2^2}\right),\ \frac{1}{S^2}\left(\frac{k_1^2\xi_1 c(\ln c)^2+k_1\xi_1 c(\ln c)k_2}{k_1^2\xi_1 c(\ln c)^2+2k_1\xi_1 c(\ln c)k_2+1-\xi_1 c-2k_2^2}\right)$$

$$=\frac{1}{S^2}\left(\frac{k_1^2\xi_1 c+k_1\xi_1 ck_2\dfrac{1}{\ln c}}{k_1^2\xi_1 c+2k_1\xi_1 ck_2\dfrac{1}{\ln c}+(1-\xi_1 c-2k_2^2)\dfrac{1}{(\ln c)^2}}\right)$$

当暴露程度$c\to 0$时，$\ln c\to-\infty$，$\dfrac{1}{\ln c}\to 0$，$\dfrac{\partial S_2^*/\partial S}{\partial S}\to\dfrac{1}{S^2}\to 0$

当暴露程度$c\to 1$时，$\ln c\to 0$，$\dfrac{\partial S_2^*/\partial S}{\partial S}\to-\dfrac{S_2^*}{S^2}\leqslant 0$

因此，当安全投资总额S非常小时，对定向攻击类型的投资分配S_2^*/S存在两种情况，当信息系统的暴露程度比较小时，对定向攻击类型的投资分配S_2^*/S和对随机攻击类型的投资分配S_1^*/S趋向于一个确定的值，不受安全投资总额S的增大或减小的影响；当信息系统的暴露程度比较大时，对定向攻击类型的投资分配S_2^*/S应随着安全投资总额S的增大而减小，而对随机攻击类型的投资分配S_1^*/S应随着安全投资总额S的增大而增大。企业在安全投资比较少的情况下，可以对定向攻击投资和对随机攻击投资按一定比例进行分配，其对安全影响不大；如果在安全投资比较大的情况下，应该随着总投资增加，加大对防御定向攻击类型的投资，减少对防御随机攻击类型的投资。

结论4：当信息系统防御随机攻击能力较强，防御定向攻击能力较弱时，在最优安全投资与网络暴露程度的关系中，面对定向攻击的最优安全投资S_2^*随着企业信息系统暴露程度的增加而减少，而对随机攻击的最优安全投资S_1^*应随着企业信息系统暴露程度的增加而增加。

令$\dfrac{\partial\phi(S_2)}{\partial S_2}=F$，即$F=k_1\xi_1 c^{k_1(S-S_2)+1}(\ln c)\dfrac{\xi_2 c}{k_2S_2+1}L-(1-\xi_1 c^{k_1(S-S_2)+1})\dfrac{k_2\xi_2 c}{(k_2S_2+1)^2}L$

$$\frac{\partial F}{\partial c}=(k_1(S-S_2)+2)k_1\xi_1 c^{k_1(S-S_2)+1}(\ln c)\frac{\xi_2}{k_2S_2+1}L+k_1\xi_1 c^{k_1(S-S_2)+1}\frac{\xi_2}{k_2S_2+1}L$$
$$+(k_1(S-S_2)+1)\xi_1 c^{k_1(S-S_2)+1}\frac{k_2\xi_2}{(k_2S_2+1)^2}L-(1-\xi_1 c^{k_1(S-S_2)+1})\frac{k_2\xi_2}{(k_2S_2+1)^2}L$$

$$\frac{\mathrm{d}S_2^*}{\mathrm{d}c}=-\frac{\partial F/\partial c}{\partial F/\partial S_2^*}=-\frac{\begin{array}{r}(k_1(S-S_2)+2)k_1\xi_1 c^{k_1(S-S_2)+1}(\ln c)\dfrac{\xi_2}{k_2S_2+1}L+k_1\xi_1 c^{k_1(S-S_2)+1}\dfrac{\xi_2}{k_2S_2+1}L\\+(k_1(S-S_2)+1)\xi_1 c^{k_1(S-S_2)+1}\dfrac{k_2\xi_2}{(k_2S_2+1)^2}L-(1-\xi_1 c^{k_1(S-S_2)+1})\dfrac{k_2\xi_2}{(k_2S_2+1)^2}L\end{array}}{\begin{array}{r}-k_1^2\xi_1 c^{k_1(S-S_2)+1}(\ln c)^2\dfrac{\xi_2 c}{k_2S_2+1}L-2k_1\xi_1 c^{k_1(S-S_2)+1}(\ln c)\dfrac{k_2\xi_2 c}{(k_2S_2+1)^2}L\\-(1-\xi_1 c^{k_1(S-S_2)+1})\dfrac{-2k_2^2\xi_2 c}{(k_2S_2+1)^3}L\end{array}}$$

$$=-\frac{\begin{array}{r}(k_1(S-S_2)+2)k_1\xi_1 c^{k_1(S-S_2)+1}(\ln c)+k_1\xi_1 c^{k_1(S-S_2)+1}\\+(k_1(S-S_2)+1)\xi_1 c^{k_1(S-S_2)+1}\dfrac{k_2}{k_2S_2+1}-(1-\xi_1 c^{k_1(S-S_2)+1})\dfrac{k_2}{k_2S_2+1}\end{array}}{\begin{array}{r}-k_1^2\xi_1 c^{k_1(S-S_2)+1}(\ln c)^2cL-2k_1\xi_1 c^{k_1(S-S_2)+1}(\ln c)\dfrac{k_2c}{k_2S_2+1}\\-(1-\xi_1 c^{k_1(S-S_2)+1})\dfrac{-2k_2^2c}{(k_2S_2+1)^2}\end{array}}$$

当$c\to 1$时，$\ln c\to 0$；当$c\to 0$，$\ln c\to-\infty$，因此，

$$\frac{\mathrm{d}S_2^*}{\mathrm{d}c}|_{c\to 1}=\lim_{c\to 1}(-\frac{k_1\xi_1c^{k_1(S-S_2)+1}+(k_1(S-S_2)+1)\xi_1c^{k_1(S-S_2)+1}\frac{k_2}{k_2S_2+1}-(1-\xi_1c^{k_1(S-S_2)+1})\frac{k_2}{k_2S_2+1}}{-(1-\xi_1c^{k_1(S-S_2)+1})\frac{-2k_2^2c}{(k_2S_2+1)^2}})$$

$$=\lim_{c\to 1}(-\frac{k_1\xi_1+(k_1(S-S_2)\frac{k_2}{k_2S_2+1}+\xi_1\frac{k_2}{k_2S_2+1}}{(1-\xi_1)\frac{2k_2^2c}{(k_2S_2+1)^2}})<0$$

$$\frac{\mathrm{d}S_2^*}{\mathrm{d}c}|_{c\to 0}=\lim_{c\to 0}(-\frac{(k_1(S-S_2)+2)k_1\xi_1c^{k_1(S-S_2)+1}(\ln c)-\frac{k_2}{k_2S_2+1}}{-k_1^2\xi_1c^{k_1(S-S_2)+1}(\ln c)^2cL-2k_1\xi_1c^{k_1(S-S_2)+1}(\ln c)\frac{k_2c}{k_2S_2+1}-\frac{-2k_2^2c}{(k_2S_2+1)^2}})$$

$$=\lim_{c\to 0}(-\frac{(k_1(S-S_2)+2)k_1\xi_1c^{k_1(S-S_2)+1}-\frac{k_2}{(k_2S_2+1)(\ln c)}}{-k_1^2\xi_1c^{k_1(S-S_2)+1}(\ln c)cL-2k_1\xi_1c^{k_1(S-S_2)+1}\frac{k_2c}{k_2S_2+1}+\frac{2k_2^2c}{(k_2S_2+1)^2(\ln c)}})$$

$$=\lim_{c\to 0}(\frac{-k_2}{k_1^2\xi_1c^{k_1(S-S_2)+1}(k_2S_2+1)(\ln c)^2cL})<0$$

由以上可以看出，随着信息系统暴露程度的增加，面对定向攻击的最优安全投资S_2^*应该减少，而对随机攻击的最优安全投资S_1^*应该逐步增加。即在企业进行一定安全投资的情况下，企业信息系统与外界联系越频繁，对随机攻击的安全投资应该逐步增加，而对定向攻击的安全投资应该减少。

（二）企业信息系统防御定向攻击能力较强，防御随机攻击能力较弱

企业信息系统防御定向攻击能力较强，防御随机攻击能力较弱，在此情形下意味着企业信息系统容易阻止定向攻击的入侵，不能阻止随机攻击的入侵，此时黑客对企业信息系统的入侵概率为：$\rho=(1-\rho_2)\rho_1=(1-\frac{\xi_2c}{k_2S_2+1})\xi_1c^{k_1S_1+1}$。等式右边表示，定向攻击入侵没能成功，但随机攻击成功入侵企业信息系统。此时企业进行安全投资的期望成本为：

$$\phi(S_1,S_2)=\rho L+(S_1+S_2)=(1-\rho_2)\rho_1L+(S_1+S_2)=(1-\frac{\xi_2c}{k_2S_2+1})\xi_1c^{k_1S_1+1}L+(S_1+S_2)\qquad(2)$$

把$S_1=S-S_2$代入（1）得$\phi(S_2)=(1-\frac{\xi_2c}{k_2S_2+1})\xi_1c^{k_1(S-S_2)+1}L+S$

结论5：当信息系统防御定向攻击能力较强，防御随机攻击能力较弱时，安全投资总额存在最大值。

结论6：当信息系统防御定向攻击能力较强，防御随机攻击能力较弱时，对定向攻击类型的投资额S_2^*应随着安全投资总额S的增大而增大，相对应地，对随机攻击类型的投资额S_1^*应随着安全投资总额S的增大而减小。

对结论1和结论2的证明如下：

$$\frac{\partial\phi(S_2)}{\partial S_2}=\frac{k_2\xi_2c}{(k_2S_2+1)^2}\xi_1c^{k_1(S-S_2)+1}L-(1-\frac{\xi_2c}{k_2S_2+1})k_1\xi_1c^{k_1(S-S_2)+1}(\ln c)L$$

$$\frac{\partial^2\phi(S_2)}{\partial S_2^2}=-\frac{2k_2^2\xi_2c}{(k_2S_2+1)^3}\xi_1c^{k_1(S-S_2)+1}L-\frac{2k_1k_2\xi_2c}{(k_2S_2+1)^2}\xi_1c^{k_1(S-S_2)+1}(\ln c)L-(1-\frac{\xi_2c}{k_2S_2+1})k_1^2\xi_1c^{k_1(S-S_2)+1}(\ln c)^2L$$

由于企业的安全投资必须有正的收益，使企业的投资边际利润不能为0，否则企业就不会进行投资，所以当$S_2=0$时，需要$\frac{\partial\phi(S_2)}{\partial S_2}\geqslant 0$，即$k_2\xi_2\xi_1c^{k_1S+2}L-(1-\xi_2c)k_1\xi_1c^{k_1S+1}(\ln c)L\geqslant 0$，因为$0<c\leqslant 1$，$lnc\leqslant 0$，很显然不等式成立。

当$c\to 1$时，$\ln c\to 0$；当$c\to 0$，$\ln c\to-\infty$，因此，

$$\frac{\partial\phi^2(S_2)}{\partial S_2^2}|_{c\to 1}=\lim_{c\to 1}(-\frac{2k_2^2\xi_2c}{(k_2S_2+1)^3}-\frac{2k_1k_2\xi_2c}{(k_2S_2+1)^2}(\ln c)-(1-\frac{\xi_2c}{k_2S_2+1})k_1^2(\ln c)^2)$$

$$=\lim_{c\to 1}(-\frac{2k_2^2\xi_2c}{(k_2S_2+1)^3})<0$$

$$\frac{\partial\phi^2(S_2)}{\partial S_2^2}|_{c\to 0}=\lim_{c\to 0}(-\frac{2k_2^2\xi_2 c}{(k_2S_2+1)^3}-\frac{2k_1k_2\xi_2 c}{(k_2S_2+1)^2}(\ln c)-(1-\frac{\xi_2 c}{k_2S_2+1})k_1^2(\ln c)^2)$$

$$=\lim_{c\to 0}(-\frac{2k_1k_2\xi_2 c}{(k_2S_2+1)^2}(\ln c)-(1-\frac{\xi_2 c}{k_2S_2+1})k_1^2(\ln c))=-\infty<0$$

因此，$\frac{\partial\phi^2(S_2)}{\partial S_2^2}|_{c\to 1}<0$，$\frac{\partial\phi^2(S_2)}{\partial S_2^2}|_{c\to 0}<0$，在此情形下，安全投资总额存在最大值。

结论7：当信息系统防御定向攻击能力较强，防御随机攻击能力较弱时，在企业信息系统成功阻止了定向攻击的入侵，但没能成功阻止随机攻击入侵的情况下，对定向攻击类型的投资分配S_2^*/S应随着安全投资总额S的增大而减小，而对随机攻击类型的投资分配S_1^*/S应随着安全投资总额S的增大而增大。

令$\frac{\partial\phi(S_2)}{\partial S_2}=F$，即$F=\frac{k_2\xi_2 c}{(k_2S_2+1)^2}\xi_1 c^{k_1(S-S_2)+1}L-(1-\frac{\xi_2 c}{k_2S_2+1})k_1\xi_1 c^{k_1(S-S_2)+1}(\ln c)L$

$$\frac{\partial F}{\partial S_2^*}=-\frac{2k_2^2\xi_2 c}{(k_2S_2+1)^3}\xi_1 c^{k_1(S-S_2)+1}L-\frac{2k_1k_2\xi_2 c}{(k_2S_2+1)^2}\xi_1 c^{k_1(S-S_2)+1}(\ln c)L$$

$$-(1-\frac{\xi_2 c}{k_2S_2+1})k_1^2\xi_1 c^{k_1(S-S_2)+1}(\ln c)^2L$$

$$\frac{\partial F}{\partial S}=\frac{k_1k_2\xi_2 c}{(k_2S_2+1)^2}\xi_1 c^{k_1(S-S_2)+1}(\ln c)L-(1-\frac{\xi_2 c}{k_2S_2+1})k_1^2\xi_1 c^{k_1(S-S_2)+1}(\ln c)^2L$$

$$\frac{\partial S_2^*/\partial S}{\partial S}=\frac{\partial S_2^*/\partial S}{S}-\frac{S_2^*}{S^2}=\frac{1}{S^2}(-\frac{\partial F/\partial S}{\partial F/\partial S_2^*}-S_2^*)$$

$$=\frac{1}{S^2}(-\frac{\frac{k_1k_2\xi_2 c}{(k_2S_2+1)^2}\xi_1 c^{k_1(S-S_2)+1}(\ln c)L-(1-\frac{\xi_2 c}{k_2S_2+1})k_1^2\xi_1 c^{k_1(S-S_2)+1}(\ln c)^2L}{-\frac{2k_2^2\xi_2 c}{(k_2S_2+1)^3}\xi_1 c^{k_1(S-S_2)+1}L-\frac{2k_1k_2\xi_2 c}{(k_2S_2+1)^2}\xi_1 c^{k_1(S-S_2)+1}(\ln c)L}-S_2^*)$$

$$-(1-\frac{\xi_2 c}{k_2S_2+1})k_1^2\xi_1 c^{k_1(S-S_2)+1}(\ln c)^2L$$

$$=\frac{1}{S^2}(-\frac{\frac{k_1k_2\xi_2 c}{(k_2S_2+1)^2}(\ln c)-(1-\frac{\xi_2 c}{k_2S_2+1})k_1^2(\ln c)^2}{-\frac{2k_2^2\xi_2 c}{(k_2S_2+1)^3}-\frac{2k_1k_2\xi_2 c}{(k_2S_2+1)^2}(\ln c)-(1-\frac{\xi_2 c}{k_2S_2+1})k_1^2(\ln c)^2}-S_2^*)$$

当$S\to\infty$时，存在两种情况：

当暴露程度$c\to 0$时，$\ln c\to-\infty$，$\frac{1}{\ln c}\to 0$，因此，

$$\frac{\partial S_2^*/\partial S}{\partial S}|_{c\to 0}=\lim_{c\to 0}(\frac{1}{S^2}(-\frac{\frac{k_1k_2\xi_2 c}{(k_2S_2+1)^2}(\ln c)-(1-\frac{\xi_2 c}{k_2S_2+1})k_1^2(\ln c)^2}{-\frac{2k_2^2\xi_2 c}{(k_2S_2+1)^3}-\frac{2k_1k_2\xi_2 c}{(k_2S_2+1)^2}(\ln c)-(1-\frac{\xi_2 c}{k_2S_2+1})k_1^2(\ln c)^2}-S_2^*))$$

$$=\lim_{c\to 0}(\frac{1}{S^2}(-1-S_2^*))\le 0$$

当暴露程度$c\to 1$时，$lnc\to 0$，因此，

$$\frac{\partial S_2^*/\partial S}{\partial S}|_{c\to 1}=\lim_{c\to 1}(\frac{1}{S^2}(-\frac{\frac{k_1k_2\xi_2 c}{(k_2S_2+1)^2}(\ln c)-(1-\frac{\xi_2 c}{k_2S_2+1})k_1^2(\ln c)^2}{-\frac{2k_2^2\xi_2 c}{(k_2S_2+1)^3}-\frac{2k_1k_2\xi_2 c}{(k_2S_2+1)^2}(\ln c)-(1-\frac{\xi_2 c}{k_2S_2+1})k_1^2(\ln c)^2}-S_2^*))$$

$$=\lim_{c\to 1}(-\frac{S_2^*}{S^2})\le 0$$

当$S \to 0$，$S_2^* \to 0$时，存在两种情况：当暴露程度$c \to 0$时，$\ln c \to -\infty$，$\frac{1}{\ln c} \to 0$，因此，

$$\frac{\partial S_2^*/\partial S}{\partial S}\Big|_{c\to 0} = \lim_{c\to 0}\Big(\frac{1}{S^2}\Big(-\frac{\frac{k_1k_2\xi_2 c}{(k_2S_2+1)^2}(\ln c)-(1-\frac{\xi_2 c}{k_2S_2+1})k_1^2(\ln c)^2}{-\frac{2k_2^2\xi_2 c}{(k_2S_2+1)^3}-\frac{2k_1k_2\xi_2 c}{(k_2S_2+1)^2}(\ln c)-(1-\frac{\xi_2 c}{k_2S_2+1})k_1^2(\ln c)^2}-S_2^*\Big)\Big)$$

$$= \lim_{c\to 0}\Big(\frac{1}{S^2}(-1-S_2^*)\Big) \le 0$$

当暴露程度$c \to 1$时，$\ln c \to 0$，因此，

$$\frac{\partial S_2^*/\partial S}{\partial S}\Big|_{c\to 1} = \lim_{c\to 1}\Big(\frac{1}{S^2}\Big(-\frac{\frac{k_1k_2\xi_2 c}{(k_2S_2+1)^2}(\ln c)-(1-\frac{\xi_2 c}{k_2S_2+1})k_1^2(\ln c)^2}{-\frac{2k_2^2\xi_2 c}{(k_2S_2+1)^3}-\frac{2k_1k_2\xi_2 c}{(k_2S_2+1)^2}(\ln c)-(1-\frac{\xi_2 c}{k_2S_2+1})k_1^2(\ln c)^2}-S_2^*\Big)\Big)$$

$$= \lim_{c\to 1}\Big(-\frac{S_2^*}{S^2}\Big) \le 0$$

由以上可以看出，当信息系统防御定向攻击能力较强，防御随机攻击能力较弱时，对定向攻击类型的投资分配S_2^*/S应随着安全投资总额S的增大而减小，而对随机攻击类型的投资分配S_1^*/S应随着安全投资总额S的增大而增大，不受网络暴露程度的影响，不同于第一种情况的结论。在此情况下，企业应根据信息系统的特点加大防御随机攻击类型的投资分配，而对防御定向攻击类型的投资分配可适当减少。

二、结论

本论文对一定预算约束下的企业网络安全投资进行了研究，在研究中主要考虑了企业网络具有不同的脆弱性，即面对黑客随机攻击与定向攻击相互结合的攻击方式，有些企业的网络系统防御随机攻击能力较强，防御定向攻击能力较弱，另一些企业的网络系统防御定向攻击能力较强，而防御随机攻击能力较弱。

第一种情形下的主要结论包括：当安全投资总额非常大的时候，对定向攻击类型的投资分配应随着安全投资总额的增大而减小，而对随机攻击类型的投资分配应随着安全投资总额的增大而增大。当安全投资总额非常小时，对定向攻击类型的投资分配存在两种情况：当信息系统的暴露程度比较小时，对定向攻击类型的投资分配和对随机攻击类型的投资分配趋向于一个确定的值，不受安全投资总额的增大或减小的影响；当信息系统的暴露程度比较大时，对定向攻击类型的投资分配应随着安全投资总额的增大而减小，相对应地，对随机攻击类型的投资分配应随着安全投资总额的增大而增大。在最优安全投资与网络暴露程度的关系中，面对定向攻击的最优安全投资随着企业信息系统暴露程度的增加而减少，而对随机攻击的最优安全投资应随着企业信息系统暴露程度的增加而增加。

第二种情况下得出的结论则与第一种情况有所不同，主要结论包括：安全投资总额存在最大值。对定向攻击类型的投资额应随着安全投资总额的增大而增大，而对随机攻击类型的投资额应随着安全投资总额的增大而减小。对定向攻击类型的投资分配应随着安全投资总额的增大而减小，而对随机攻击类型的投资分配应随着安全投资总额的增大而增大。

本论文重点研究了企业面对组合攻击下的安全投资，研究结果可以为企业的网络安全投资提供参考，企业可以根据网络系统的技术特点及与外界的联系频繁程度进行合理的投资分配。

参考文献

[1] GAO X, ZHONG W. Information security investment for competitive firms with hacker behavior and security requirements[J]. Annals of Operations Research, 2015, 235(1): 277-300.

[2] WU Y, FENG G, WANG N, et al. Game of information security investment: Impact of attack types and network vulnerability[J]. Expert Systems with Applications, 2015, 42(15): 6132-6146.

(下转第99页)