信息安全风险管理绩效研究

卢志刚[1,2] 潘 林[1,2] 刘宝旭[1] 许榕生[1] 蒋文保[3]

(中国科学院高能物理研究所计算中心 北京 100049)[1]

(中国科学院研究生院 北京 100049)[2] (北京信息科技大学 北京 100101)[3]

摘 要 分析了当前风险管理的现状和所面临的问题,并通过风险确认,提出了一个风险管理效率判别模型,以对风险管理方案进行判别,找出最佳的风险管理方案。通过分析进一步指出了基于信息资产提供业务的风险管理投资和安全事件损失的联系,并对其有效性进行了验证。实验结果表明,此方法是行之有效的。

关键词 信息安全,风险管理,方案决策,绩效

Study on Performance of Information Security Risk Management

LU Zhi-gang[1,2] PAN Lin[1,2] LIU Bao-xu[1] XU Rong-sheng[1] JIANG Wen-bao[3]

(Computing Center, Institute of High Energy Physics, Chinese Academy of Sciences, Beijing 100049, China)[1]

(Graduate of University, Chinese Academy of Sciences, Beijing 100049, China)[2]

(Beijing Information Science & Technology University, Beijing 100101, China)[3]

Abstract Analyzed the situation and likely problems of the current risk management through affirming the current risk, combined with analysis of financing final accounts, and then put forward a systematic and normative differentiating model for the efficiency of risk management to distinguish the risk management projects from which found out the optimal one. Then pointed out the link between the investment of risk management and the loss of security incidents through further analyzing base on business, and gave out the verification of its effectiveness. The result of verification shows that this model is effective.

Keywords Information security, Risk management, Decision-make, Performance

随着信息技术的发展,以网络为载体、以信息资源为核心的信息系统规模不断扩大,随之而产生的是信息和网络攻击事件的频繁发生和不断升级,信息系统所面临的安全风险和威胁日趋严重。要解决网络信息系统的安全问题,首先就要了解信息系统存在的安全隐患与面临的威胁,充分评估这些威胁可能带来的风险[1]。

风险管理(Risk Management)是一个动态的过程,它包括风险识别、风险分析、风险评估和风险控制等内容。这是一个不断降低安全风险的过程,其最终的目的就是使系统的残余安全风险降低到一个可以接受的程度。安永(Ernst & Young)在"第10年度全球信息安全调查报告"指出,多年来,信息安全曾被看作是IT开销并妨碍有效运行。现在,有更多的人(82%)认为信息安全已经成为企业运行的正面贡献者,为企业带来利益,并且改善了信息技术整体的运行效率。近几年,组织内部的风险评估与安全管理越来越为政府、企业所重视,出现了大量的评估标准和评估工具。目前常用的一些标准有国际标准化组织制定的ISO/IEC1779[2]、英国Insight Consulting公司的CRAMM[3]风险评估工具、美国Risk Watch公司开发的安全风险管理软件Risk Watch ISO17799[4],它们都完全遵照ISO17799规范,具有风险评测和风险管理功能。但实施信息安全风险管理的成功率却非常低。The Standish Group调查表明,截至2008年,各企业和部门用于信息安全方面的投资在逐年上升,而信息安全风险管理项目的成功率普遍都在30%以下[5]。因此,针对资产自身情况,制定出最优的风险管理实施方案,具有重要的实际意义。

1 系统风险管理绩效评判

已有的信息系统风险管理方法主要集中在从技术层面制定控制信息系统安全风险的安全解决方案,对基于风险管理的信息安全投资水平的绩效和最优化领域则少有研究。传统的投资决策主要是基于成本-效益分析进行的,信息系统安全投资的成本-效益难以完全用货币价值度量,因此信息系统风险管理相对于传统项目的绩效决策有着一定的特殊性。

现在关于风险管理和风险评估的标准层出不穷,执行不一样的标准。对需要进行或有意向进行风险管理和风险评估的管理人员,如何选择合适风险管理方法,成了一个亟待解决的问题。风险管理决策或管理人员在选择和评估风险管理方案阶段会出现决策困难,无法确定是否应该进行风险管理,无

到稿日期:2009-07-07 返修日期:2009-09-09 本文受国家科技支撑计划重点项目(2009BAH52B06),北京市自然科学基金面上项目(4072010)资助。

卢志刚(1983-),男,博士生,E-mail:luzg@ihep.ac.cn;潘 林(1984-),男,博士生;刘宝旭(1972-),男,博士,副研究员;许榕生 研究员,博士生导师;蒋文保 副教授。

法决定风险管理前的投资预算和方案选择，更无法预见进行风险管理所能带来的实际利益，即风险管理绩效。

在风险管理领域一直都存在的问题，就是如何合理有效地评估信息安全风险管理的绩效，在风险投资和投资回报上找到一个好的平衡点，使信息资产获得最大的投资回报。本文的目的就是给出一个方法，用来显示风险管理本身所具有的价值，衡量风险管理所带来的效益。

2 信息安全风险管理绩效模型

2.1 当前风险确认

风险分析中要涉及资产、威胁、脆弱性3个基本要素，每个要素都有各自的属性。资产的属性是资产价值；威胁的属性可以是威胁主体、影响对象、出现频率、动机等；脆弱性的属性是资产弱点的严重程度。要进行风险管理，首先要做好3个方面的准备，从而对当前的风险状况有一个准确的认识。这3个方面分别就是我们说的风险管理中3个基本要素的识别：资产识别、脆弱性识别和威胁识别。

当前风险确认包含两个方面：

1)根据威胁及威胁利用脆弱性的难易程度判断安全事件发生的可能性，用 p 表示。p 是关于信息安全投资 Z、资产的脆弱性 v 和资产面临的威胁 t 的函数。

2)根据脆弱性的严重程度及安全事件所作用的资产的价值计算安全事件发生后造成的损失(如图1所示)，用 L 表示。

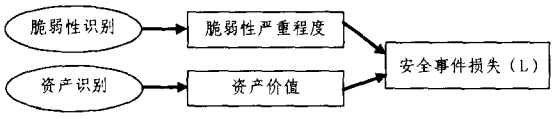

图1 安全事件损失确认

2.2 信息安全风险管理绩效评估

需要进行风险管理的企业或者部门所要达到的目的就是降低安全事件发生的可能性和安全事件发生造成的损失，从而降低风险值。要达到这个目的，就需要对信息安全进行投资。在信息安全上增加投资会导致风险级别的降低，信息安全上投资的减少会导致风险级别的升高，这两者存在一定的对应关系。Klerk[6]曾经提出过一个由风险投资额度 x 作为自变量、投资绩效 u 为变量的关系模型 $u(x)=1-e^{-x/\rho}$。本文发现其模型的推导和验证存在一定的误差。在其研究的基础上，本文根据合理推导，提出一个风险管理绩效函数为 $u(x)=a-\frac{1}{\rho}e^{-x/\rho}$，并对其有效性进行了验证[7]，指明了信息安全风险管理投资量 x 与投资绩效 u 之间的函数关系。其中引入风险损失最大承受限度值 ρ[6]表示风险管理方案决策者对风险发生时造成损失的容忍阈值，a 为绩效修正值。引用文献[6]的论证，令 $a=1$。

资产损失可以划分为两个部分：一部分为安全时间发生后的损失，另一部分为风险管理费用。前期风险确认中资产发生概率 p、资产花费如表1所列。

表1 资产信息安全损失划分

资产损失	概率	价值
X	p	Z+L
	1−p	Z

由此，资产的信息安全损失所造成的绩效可以描述为

$$u(X)=p*u(Z+L)+(1-p)*u(Z) \tag{1}$$

对于信息资产，要使风险管理投资取得最大绩效，等同于使信息资产损失绩效最低，$u(X)$ 取得最小值，$\partial u/\partial Z=0$。展开得

$$\frac{\partial u}{\partial Z}=\frac{\partial[p(Z,v)\cdot u(Z+L)+(1-P(Z,v))\cdot u(Z)]}{\partial Z}$$

$$=\frac{1}{\rho}+(1-e^{-L/\rho})(\frac{\partial p_Z(Z,v)}{\partial Z}-\frac{p(Z,v)}{\rho})=0 \tag{2}$$

式中，$0<v<1$。

2.3 风险管理投资回报

Gordon[8]描述风险发生概率 p 与前期确认的信息资产的威胁 t 和脆弱性 v 以及用于信息安全风险管理的投资 Z 都有一定的相关性，描述为 $p=p(Z,v,t)$。

$p=p(Z,v,t)$ 是关于 Z 和 v 的可微单调函数，随着 Z 的增加，伴随着 v 的减少，风险管理实施者通过提高 Z 来降低资产风险，最终达到降低安全事件损失的目的。因此 $v-p(Z,v,t)$ 表述了投资 Z 所带来的资产脆弱性的降低。考虑系统的威胁 t 以及当风险事件发生时信息资产的损失 L，风险管理投资 Z 所获的收益函数可以描述为：

$$BENEFIT(Z)=(v-p(Z,v,t))tL \tag{3}$$

Hoo[9]在其文章中提出风险管理 RoI (Return on Investment)，即风险管理投资回报，RoI=Return−Investment。本文中的风险管理投资回报如下：

$$RoI(Z)=BENEFIT(Z)-Z \tag{4}$$

即

$$RoI(Z)=(v-p(Z,v,t))tL-Z \tag{5}$$

风险管理的最终目的就是要获取最大的投资回报，即 $RoI(Z)$ 的最大值。$p=p(Z,v,t)$ 是关于 Z 的可微函数，因此 $RoI(Z)$ 同样关于 Z 可微，当 $\partial RoI(Z)/\partial Z=0$，$RoI(Z)$ 达到其函数值的最高点，风险管理投资也得到最大的投资回报，如下所示：

$$\partial ROI(Z)/\partial Z=\partial[(v-p(Z,v,t))tL-Z]/\partial Z=0 \tag{6}$$

化简后可得

$$\partial p/\partial Z=-v/(Z+1)^2\cdot L\cdot t \tag{7}$$

对式(7)进行对于 Z 的积分，可得 $p(Z,v,t)$ 关于 Z 的函数：

$$p(Z,v,t)=v/[(Z+1)Lt]+k,0<k<1-v \tag{8}$$

对信息资产而言，其所面临的威胁 t 是外部因素，t 的值不会随着风险管理而发生改变，在这里定义 t 为常数，且 $0<t<1$。

2.4 信息安全风险管理绩效计算模型

由2.2节和2.3节分析，当信息资产风险管理投资获得最大绩效时，满足 $\partial u/\partial Z=0$，即式(2)；信息资产风险管理投资获得最大投资回报 $RoI(Z)$ 时，可得 $p(Z,v,t)$ 关于 Z 的函数满足式(8)。

当信息资产进行风险管理获得最大绩效时，风险管理投资量 Z 和信息资产安全事件损失量 L 满足式(1)与式(7)连立式(1)与式(7)求解，可得如下的绩效关系模型：

$$\frac{\rho v}{(Z+1)^2\cdot Lt}+\frac{v}{(Z+1)\cdot Lt}+\frac{1}{e^{-L/\rho}-1}+k=0 \tag{9}$$

令 $Z/L=D$，D 为绩效最高的风险管理投资量与预期损失的比率，则式(9)可表达为

$$\frac{\rho v}{(D+1/L)^2\cdot L^3t}+\frac{v}{(D+1/L)\cdot L^2t}+\frac{1}{e^{-L/\rho}-1}+k=0 \tag{10}$$

令 R 为所有决策方案的集合，$D_i \in R$ 表示第 i 个决策方案，得到对于风险管理方案 D_i 所对应的安全事件损失 L_i 的变化。决策者所能承受的风险最大承受阈值变化时，最佳投资额度与损失比率 D_i 也会发生变化，比率 D 和安全事件损失 L 的绩效关系模型 EFFI(D_i)满足：

$$\frac{\rho v}{(D_i+1/L_i)^2 \cdot L_i^3 t}+\frac{v}{(D_i+1/L_i)\cdot L_i^2 t}+\frac{1}{e^{-L/\rho}-1}+k=0 \tag{11}$$

式中，$0<v,t<1$，$0<k<1-v$。

在模型决策中，多专家经验是要考虑的因素。对于信息资产当前的风险状况参数 v 以及风险最大承受限度值 ρ 等参数，在模型的计算中引入泊松(Poisson)函数来解决多专家经验协同问题，可以在专家经验相差较大的情况下有效用方差减小模型的震荡，并且此方法在实验过程中用 MATLBA 仿真可以进行模拟。假设 x 为需要结合多专家经验决定的参数，则

$$x=\sum_{i=1}^{n} RANDPOSSON(x_i)\cdot l_i$$

式中，l 为某位决策专家在此决策体系中的权重值，且 $\sum_{i=1}^{n} l_i=1$。具体的权重决定因素可以通过专家对信息资产的熟悉程度、重要性程度来决定。

3 有效性验证

根据信息安全风险管理和信息安全风险值以及信息资产的脆弱性和威胁间的属性关系，可以对关系模型做合理性验证。

本文模型中包含两部分主体内容，即风险管理绩效函数和投资回报最优引出的 Z 与 v 的函数关系式：$p(Z,v,t)=v/[(Z+1)Lt]+k(0<k<1-v)$。其中绩效理论已经比较成熟，作者将其引入到风险管理绩效评判中，且在作者的其它文献中已经证明其合理性。因此，模型有效性验证的核心就是证明函数关系式 $p(Z,v,t)$ 的合理性。k 为由专家经验决定的常数，信息资产威胁 t 为常数，且都和 Z,v 相互独立，在模型验证过程中无需考虑。现记关于 Z 和 v 的函数 $F(Z,v)=v/(Z+1)Lt$，$0<t,v<1$。Gordon 在其文献中曾经提出风险管理各要素之间的自然属性联系，通过分析，可以验证 $F(Z,v)$ 满足定理 1－定理 4。

定理 1 对于 $Z\in(0,\infty)$，

$$\frac{dF(Z,v)}{dZ}|_{Z=Z_1} > \frac{dF(Z,v)}{dZ}|_{Z=Z_2} \quad (Z_1<Z_2)$$

随着风险管理投资的增加，同等量的投资所取得的风险级别的降低将会越来越小。

定理 2 当 $Z\to\infty$，

$\lim F(z,s)\to 0$

随着用户风险管理投资的大量增加，风险的级别会随之不断降低，直至无限接近于 0，信息资产不存在任何风险。

定理 3 对于所有的 v，满足

$F(0,v)=v/a$

a 为比例系数。

信息资产用于风险管理的投资 $Z=0$ 时，资产的风险级别将会保持现在的水平不变。

定理 4 对于所有的 Z，满足

$F(Z,0)=0$

当信息资产脆弱性为 0，即足够安全时，是没有必要对信息资产进行风险管理的，任何数量的风险管理投资都不会导致资产安全性的变化。

结合所分析得出的对应关系，可见根据最佳风险管理投资回报推导出的 $F(Z,v)$ 函数关系能够满足信息安全风险管理各要素之间的属性关系，为模型的准确性和可靠性提供了佐证。

4 仿真结果

文献[8,10]采用基于风险可变的动态模型，最后证明最佳风险投资额度不会超过风险预期损失量的 36.8%，但在文献[10]中缺乏对风险损失最大承受限度值 ρ 的考虑。在实验中，Z,L,ρ 在实际模型中采用同样的度量单位，以信息资产的自身价值为单位 1。在实验中，采用 MATLAB7.0 对模型进行仿真模拟，分别考虑信息资产值 $\rho=0.15$，$\rho=0.4$ 以及 $\rho=0$ 时得出伴随着信息安全事件损失 L 的变化，在获得绩效最高的风险管理投资的情况下比率 D 的变化情况。信息资产脆弱性 v 的值采用文献[8]中的实验数据，令 $v=0.2$。ρ 的值考虑专家经验，在实验程序中，假设有 10 个专家，在 MATLAB 中用泊松分布函数模拟专家经验的偏差，验证程序算法如下所示：

```
start
    tiny=1000;
    expert=10;
    rho=poissrnd(rho * tiny,1,expert)/tiny;
    v=poissrnd(v * tiny,1,expert)/tiny;
    t=poissrnd(t * tiny,1,n expert)/tiny;
    k=poissrnd(k * tiny0,1,expert)/tiny;
    solve('rho0 * v0/((D+1/L0)^2 * L0^3 * t0)+v0/((D+1/L0) *
L0^2 * t0)+1/(exp(-L0/rho0)-1)+k0','D') //模型求解
    get:D1,D2;(舍去解 D2)
    dL=绘图步长精度;
    L=dL:dL:1;
    for i=1:nmax
        for j=1:length(L)
            L0=L(j);
            D1(j,i)=解 D1;
    plot(L,D1(:,i)) //绘图
end
```

MATLAB 中泊松函数 poissrnd 给出的是整数随机数，所以计算中做了处理，将值本身放大到整数，求出随机数后再做归一化。程序中的 tiny 反映了该过程的精度，值越大精度越高。

在 $F(Z,v)$ MATLAB 方程求解中，出现了对称解 $D1$ 和 $D2$。因为 D_i 负值没有意义，将 $D2$ 舍去。

从分析实验结果得出，风险投资效率趋势与文献[8]基本符合。当 ρ 为 0.15 时，预期风险损失占信息资产价值小于 5.7%或大于约 47%时风险投资是毫无意义的。随着容忍阈值 ρ 的增加，信息资产管理者对于风险损失的敏感程度是降低的，最佳的投资比率会向高点偏移。对 ρ 值进行不同赋值后，此假设是可以验证的。ρ 为 0.4 时，优风险管理投资量约 $0.14<Z<0.55$。分析后发现，风险损失的容忍阈值的改变决定着最佳风险投资量的趋势。随着 ρ 值的增加，风险管理投

(下转第 55 页)

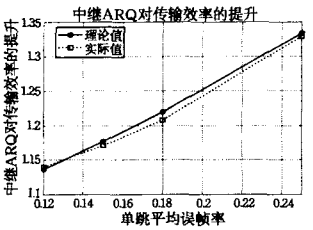

图 12　理论值与仿真结果的对比

结束语　本文用部分窗口多拒绝 ARQ 为终端节点设计了 RLC 子层，并用中继 ARQ 的概念为中继节点设计了 RLC 子层。根据超宽带无线网络的应用背景和特点，用马尔可夫链为仿真建立了误帧模型，按照误帧模型参数取值的不同进行了仿真。仿真结果显示，使用中继 ARQ 能提升 RLC 子层吞吐率，降低 SDU 时延。随后分析了单跳误帧率增加对平均吞吐率和发送方带宽有效利用率的影响，并通过仿真结果的对比进行了验证。

本文只对两跳网络收发数据的场景进行了仿真，且中继节点和终端节点分工明确。但在实际的个域网(WPAN)中，每一个多媒体电子设备都需要具有数据收发的能力，而且单独存在的中继节点并不能最大限度地发挥其作为一个电子设备带给人们的便利，因此还可以进一步设计针对多跳网络的、能将中继节点和终端节点融合的 RLC 子层方案，并仿真多个用户同时收发数据的场景。

参 考 文 献

[1] Xiao Yang, Shen Xuemin, Jiang Hai. Optimal ACK Mechanisms of the IEEE 802. 15. 3 MAC for Ultra-Wideband Systems[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(4): 155-156

[2] 武汉汉网高技术有限公司. 多拒绝自动请求重传 ARQ 方法[R]. 中国. 应用型, 02115845, 2004: 7-35

[3] 吴伟民. B3G 系统数据链路层研究[D]. 武汉: 华中科技大学, 2006

[4] Otsuki, Hideki, Yamaoka, et al. A proposal of adaptive protocol relay capability for real-time media with allowable delay[J]. Electronics and Communications in Japan, Part I: Communications, 2005, 88(8): 50-59

[5] Oyman O. End-to-end throughput and latency measures for multi-hop routing in relay-assisted broadband cellular OFDM systems[R]. Long Beach, CA, United States, Institute of Electrical and Electronics Engineers Computer Society, Piscataway, NJ 08855-1331, United States, 2007

[6] Wiemann H, Meyer M, Ludwig R, et al. A novel multi-hop ARQ concept[R]. Stockholm, Sweden, Institute of Electrical and Electronics Engineers Inc., Piscataway, NJ 08855-1331, United States, 2005

[7] Cramer R J, Scholtz R A, Win M Z. Evaluation of an Ultra-wideband Propagation Channel[J]. IEEE Transactions on Antennas and Propagation, 2002, 50(5): 561-570

[8] Zhang R, Cai L. A Markov model for UWB indoor channel with shadowing[C]// International Conference on Quality of Service in Heterogenous Wired/Wireless Networks. 2007

[9] Saleh A, Valenzuela R. A Statistical Model for Indoor Multipath Propagation[J]. IEEE JSAC, 1987, SAC-5(2): 128-137

[10] 陈敏. OPNET 网络仿真[M]. 北京: 清华大学出版社, 2006

(上接第 42 页)

资额度区间向高点偏移，这说明随着容忍阈值的增加，将伴随着风险投资可能性的减少。考虑一种极端的情况，信息资产的容忍阈值 ρ 为无穷大时，通过分析可以看出，此时对于信息资产的任何风险管理投资都是毫无意义的。图 2 给出风险管理最佳投资量。

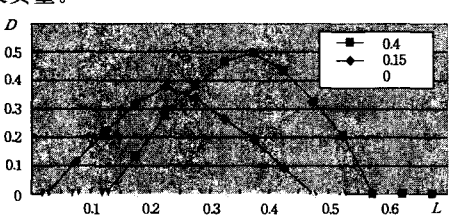

图 2　风险管理最佳投资量

综合分析结果以及文献[8,10]的综合比较，本模型能够准确描述出风险管理预期损失与最佳绩效信息安全投资量的关系，是行之有效的。

结束语　本文将绩效理论引入到风险管理中，利用风险管理绩效函数和由风险管理投资回报最优引出的风险管理投资与信息资产风险的函数关系式得出风险管理绩效计算模型，评价信息资产进行风险管理方案的合理性，并进行了合理性验证。

本文还有待进一步研究的工作包括：(1)对于不同业务资产的容忍阈值的计算没有标准的计算模型，这对于本文关系模型的准确性造成了一定的偏差；(2)在本文中，对于信息资产的预期风险损失也只是采用了文献中的现有数据，在实际问题的研究中，这是进行风险管理效率研究的重要内容，合理的风险损失预测对本文的关系模型乃至于整个信息安全风险管理领域都会产生比较大的现实意义。

参 考 文 献

[1] 冯登国，张阳，张玉清. 信息安全风险评估综述[J]. 通信学报，2004，25(7)：10-18

[2] ISO/IEC 17799, Information Technology-Security Techniques-Code of Practice for Information Security Management [S]

[3] CRAMM. Managing CRAMM Reviews Using PRINCE [EB/OL]. http://www.cramm.com, 2005-10-13

[4] COBRA. Framework for Cumulative Risk Assessment [EB/OL]. http://www.riskworld.com, 2003-5-27

[5] Standish Group International. Trends in IT Investments [EB/OL]. http://www.marketresearch.com/, 2008

[6] de Klerk, Antonie M. The Value of Project Risk Management [C]//Portland International Conference on Management of Engineering and Technology. IEEE, July-August 2001: 570-576

[7] Lu Zhigang. Study on Efficiency of Risk Management for Information Security Based on Transaction[C]// Second International Symposium on Electronic Commerce and Security. IEEE, 2009: 1006-1011

[8] Gordon L A. The Economics of Information Security Investment [J]. ACM Transactions on Information and System Security, 2002, 5(4): 438-457

[9] HOO K. How much is enough? A risk-management approach to computer security[D]. Consortiumfor Research on Information Security Policy (CRISP) Working Paper. Stanford, Calif: Stanford University, June 2000

[10] Huang C D, Hu Qing. An economic analysis of the optimal information security investment in the case of a risk-averse firm[J]. Int. J. Production Economics, 2008, 114, 793-804