效用函数在 IT 风险评估中应用

Utility Function Usage in IT Risk Evaluation

赵志策 张 蕾 （石家庄经济学院 职业技术学院;河北省广播电视大学直属学院 河北 石家庄 050021）

摘 要: 把效用函数引入 IT 风险评估领域,利用效用函数反函数,定义绝对损失效应和相对损失效应,并用以度量安全风险;在此基础上建立了统一的风险等级划分标准。绝对损失效应能度量高损失、低概率与低损失、高概率风险事件间差异,相对损失效应能度量不同规模组织风险承受能力差异,而普遍使用的平均损失却不能度量这些差异。

关键词: 信息安全 风险评估 效用函数 损失效应

信息安全风险评估在安全体系建设中时非常重要一个阶段,国内公安部、银监会和信息安全测评中心等部门都在积极推进 IT 风险评估方面的工作。目前在风险评估度量方面,定量方法较少,多采用半定量半定性方法,而其理论基础往往是根据平均损失大小或信息资产的通用平均价值来度量风险大小和风险的损失大小,而平均损失不能比较高损失、低概率与低损失高概率风险间的差异,而实际上前者风险更大,这体现了人们的对高风险的回避,再有平均损失不能反映不同规模组织对同样损失的风险承受能力的不同,本文拟采用效用函数理论提出一种新的度量方法。

效用函数理论在保险精算领域有着很好的应用,在资源适配领域也有应用。本文把效用函数理论引入到 IT 风险评估领域,提出了一种基于效用函数的风险度量方法 这一方法利用效用函数的反函数,引入绝对损失效应和相对损失效应并把它们用以度量安全风险,绝对损失效应克服了平均损失不能度量高损失、低概率与低损失高概率风险间的差异 相对损失效应克服了不同规模组织对同样大小损失风险承受能力的差异,在此基础上我们建立了统一的 IT 风险等级划分标准。

1 效用函数介绍

效用本意是一种主观感受,是一种主观愿望的满意程度 效用函数是对效用的一种数量表示,给出了综合满意程度的数量度量 其定义如下：

定义 1 集合 M 上的实值函数 $x(\varphi)$ 若满足条件 $\varphi \geqslant \varphi(y) <=> x \geqslant y$,则称 $(\varphi(x)$ 为集合 M 上的效用函数。

效用函数理论在保险精算领域有着很好的应用,是保险费计算的重要理论基础,其中财富效用是主要讨论的话题,若 x 为财富,则根据效用函数理论,效用函数应满足以下两个性质：

i) $\varphi(x)$ 是 x 的单调增函数(即财富增加满意度增加)

ii) $\Delta\varphi = \varphi(x+\Delta x) - \varphi(x)$ 是 x 的单调减函数(对于同样的增量 Δx,随财富 x 的增加,所增加的效用 $\Delta\varphi$ 减少),这一性质称为边际效用递减规律。若 $\varphi(x)$ 具有二阶导数,则以上性质可表示为：

$$\varphi'(x) > 0 \qquad \varphi''(x) < 0$$

2 评估 IT 风险的效用函数方法

根据 ISO/IEC13335,风险为威胁利用组织的一个或一组脆弱点对组织造成损害的潜在,资产、威胁、脆弱点共同构成风险的三要素。资产指任何对组织有价值的东西,其中包括物理资产、软件、数据、提供服务的能力、无形资产(声誉、形象)等,这都是需要保护的对象。风险导致的损失可以在以上资产的破坏上得以体现。

IT 风险评估主要在威胁、脆弱点标识的基础上,分析组织可能面临的不期望发生的事件 并计算不期望发生的事件发生的可能性大小及其造成的影响,然后

采用一定的办法来度量风险,如给出风险等级;最后根据风险评估的结果选取适当的防护措施。本文中风险由以下一系列有序对表示:

risk≡ {(E1, L1),…,(Ei, Li),…,(En, Ln)},

其中 Ei (i =1,. . . , n) 是一系列不期望发生的事件,Li (i =1,. . . , n) 是一系列不期望发生事件的发生的可能性。

我们认为,风险造成的损失可由资产价值及损失份额(比例)来度量,需要注意的是,这里的资产泛指一切对组织有价值的东西(包括服务能力,声誉等),为度量损失,我们首先需进行资产评估,识别关键资产;假设组织经资产评估后,有 m 个关键资产,其价值分别为 VAj (j =1,. . . , m),又假设 Ei(i =1,. . . ,n) 对第 j 个资产造成的损失份额为 Partij(i =1,. . . ,n ;j = 1,. . . , m),没有损失则 Partij =0,于是;

Ei 造成的损失为 $Loss_i = \sum_{j=1}^{m} \mathrm{Part}_{ij} \times VA_j$

系统总的期望损失为 $Loss = \sum_{i=1}^{n} Loss_i \times L_i$

2.1 绝对与相对损失效

在以期望损失为风险度量标准的模型中,高损失、低可能性事件与低损失、高可能性事件是不能区分的,比如某两事件导致的损失及发生可能性分别为:1000 万元,1/1000 的可能性和 10 万元,1/10 的可能性,两者的期望损失相同,能否说两者造成风险相同,这自然是不合理的,前者有更大风险。再有同样大小的损失对不同规模的公司造成的风险也不同。基于期望损失的以上局限性我们提出绝对损失效应与相对损失效应。

本文中,拟采用效用函数来度量损失带来的不满意程度(称为损失效应),设 x 为损失,μ(x)为它带来的不满意程度,根据人们的习惯,μ(x)应满足:μ(x)′ > 0 μ(x)′′ > 0

μ(x)′表示损失增加使得不满意度增加,μ(x)′′表示不满意程度随着损失 x 的增加其增加速度加快,这体现了人们心里承受能力,这一点在上面提到的两种风险事件(1000 万元损失,1/1000 的可能性和 10 万元损失,1/10 的可能性)中的以体现,1000 万元损失带来的损失效应不能简单看成 10 万的 100 倍,而是比 100 倍更大。显然效用函数不满足 μ(x)的性质,但由数学知识可知,效用函数的反函数满足这种性质,因而可令 μ(x) =φ-1 (x),其中 φ(x)为一效用函数。

定义不期望发生事件 Ei 造成的绝对损失效应为 LossUi =μ(Lossi),而相对损失效应则是对相对损失计算效用,需计算损失在总资产中所占比例,然后再计算其效用,根据前面的假设组织总资产为

$$GrossV = \sum_{j=1}^{m} VA_j$$

Ei 造成的相对损失效应为

$$R\_LossU_i = \mu(Loss_i / GrossV)$$

由于 Ei 发生的可能性大小不同,因而需计算期望损失效应。期望绝对损失效应为

$$LossU = \sum_{i=1}^{n} \mu(Loss_i) \times L_i$$

期望相对损失效应为

$$R\_LossU = \sum_{i=1}^{n} \mu(Loss_i / GrossV) \times L_i$$

由保险领域的经验可知,效用函数能反应人们对财富的偏好,其反函数能反应人们对风险的回避,可以作为损失带来不满意程度的度量,绝对损失反应的是一定的绝对损失对组织造成的不满意程度,因而绝对损失效用是风险造成组织总的不满意程度的度量,其值越大,不满意程度高,风险就大,反之则小。它适于度量一个公司风险的大小,风险大小可在绝对损失效应值上得以体现。我们还可以通过以下方程来计算组织面临的不确定的损失转化为某一同等效应的固定损失的风险:

$$\mu(x) = \sum_{i=1}^{n} \mu(Loss_i \times L_i)$$

由以上方程解出 x(如 x =100 万),则我们可以说组织面临的风险,在绝对损失效应的意义下,与直接损失 x =100 万相同,也就是说组织面临的损失所能带来的不满意度与直接损失 x 带来的不满意度相同,前面的 Lossi 是随机损失,而 x 是固定损失,这一转化对方便领导决策是很有价值的。

相对损失效用反应的是某一比例的损失对组织造成的不满意程度,与绝对损失效用一样,其值越大,不满意度越高,风险越大。与绝对损失不同的是它使用相对损失计算效用,与组织的规模无关。仿绝对损失效用,通过

以下方程,把随机损失转化为固定损失:

$$\mu(y) = \sum_{i=1}^{n} \mu(\mathrm{Loss}_i / \mathrm{GrossV}) \times \mathrm{L}_i$$

由以上方程解出 y(比如说 y = 20%),我们可以说,在相对损失效用的意义下,组织面临的风险与损失公司总资产的 20% 相同,与绝对损失不同的是,前面解出的是绝对损失 x,它对不同规模的公司带来的不满意程度不同,此处解出的是相对损失 y,可以大致认为它给不同公司带来的不满意度相同,因而便于制定统一的风险度量标准,因为由以上方程解出的 y 有固定的范围[0,1],损失比例高于 1 时做破产处理,与 y = 1 效果相同,我们可以把[0,1]区间划分为若干段,相应表示不同的风险等级。

2.2 指数效用函数及应用举例

效用函数理论的关键是效用函数,选取一能真实度量人们满意程度(或不满意程度)的效用函数是我们的关键所在,指数效用函数在保险精算中有广泛的应用,是保费计算的基础,此处我们仍使用指数效用函数,其表达式为

$\phi(x)=\frac{1}{a}(1-e^{-ax})$ a > 0 为常数,表示对风险的厌恶程度。

其反函数为 ,易知 $\mu(x)=-\frac{1}{a}\ln(1-ax)$,当 μ(x) > 0 a = 0 时 , $\lim_{a\to 0}\mu(x)=-\lim_{a\to 0}\frac{\ln(1-ax)}{a}=-\lim_{a\to 0}\frac{-x}{1-ax}=x$

此时由方程 $\mu(x)=\sum_{i=1}^{n}\mu(Loss_i)\times L_i$

可解出 $x=\sum_{i=1}^{n}Loss_i\times L_i$

,实际上 x 就等于期望损失,因而基于期望损失的度量方法是该方法当 a = 0 时的特例。对于下面的三种风险事件(1000 万元损失,1/1000 的可能性、100 万元损失,1/100 的可能性和 10 万元损失,1/10 的可能性),我们用方程

$$\mu(x)=\sum_{i=1}^{n}\mu(Loss_i)\times L_i$$

分别给予求解(此时 n = 1)出该事件相当的固定损失(单位万元):

a = 0.0009 时相当的固定损失分别为 :2.5555 1.0474　1.0041

a = 0.0001 时相当的固定损失分别为 :1.0535 1.0050　1.0005

a = 0 时相当的固定损失全为 1。

从上例可以看出 a = 0 时,三者结果相同,实际就是期望损失,a 越大,计算出结果越大,且高损失风险计算值增加更快,如 a = 0.0009 时,1000 万元损失,1/1000 的可能性的风险相当于 2.5555 万的损失,远大于其平均损失 1 万元,这体现出人们对高风险的回避。

同样地,若知道组织的关键资产价值、可能发生的不期望发生的事件等相关信息,利用指数效用函数及相对损失效应理论可以计算出组织所面临风险所相当的相对损失值。

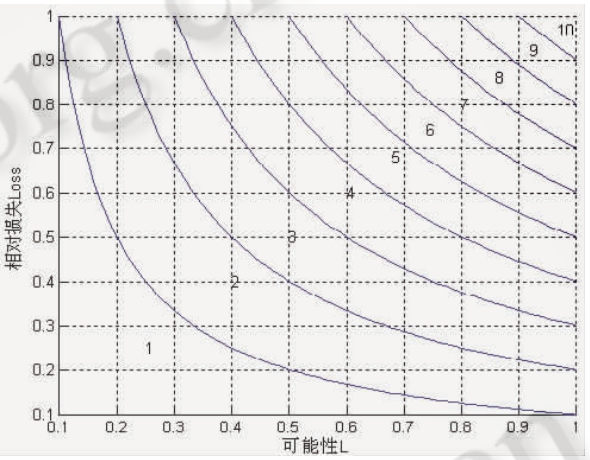

图 1　基于期望损失的风险等级划分

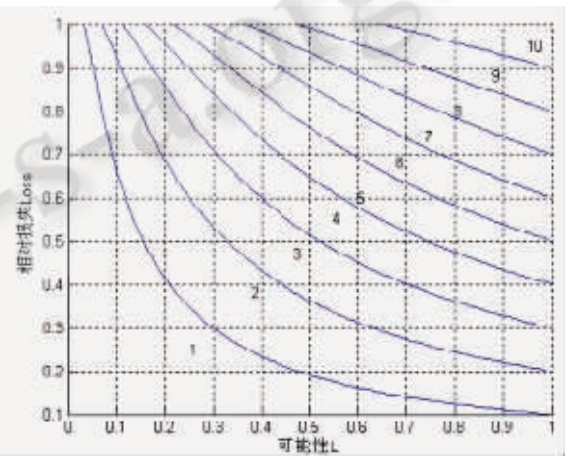

图 1　基于指数损失的风险等级划分

3　指数效用模型划分风险等级

风险评估中经常需要根据事件 E 造成的损失 loss 和其发生的可能性 L 划分等级,当把 loss 表示成相对损失时,其值在[0,1]区间上,L 值也同样。若依据期望损失理论,我们将根据 loss × L 值大小划分等级,结

果见图1 根据前面提到的相对损失效应理论,采用指数效用函数(a =0.95),

由方程 $\mu(y) = \mu(loss) \times L$

解出的 y 在[0,1] 区间上,依据 y 值大小,我们可建立风险等级划分方法,结果见图 2。图中虚线是坐标网格线,数字表示它所处区域的风险等级,值越大,风险越大,最大级别为 10 级。从两图比较可以看出,两者对于高损失风险处理上是不同的,如相对损失为1,可能性为 0.45 的事件在期望损失的等级划分方法下是 5 级风险,而依据指数效用划分方法是 8 级风险;另外,可能性为 1,损失为 0.45 的事件在两种方法下都是 5 级风险,指数效用方法中体现了这两种事件的风险差异,而期望损失理论不能发现这一差异,这体现了指数效用风险等级划分方法的优越性。

4 总结

风险定量评估方法的优点是用直观的数据来表述评估的结果,而且比较客观。定量分析方法的采用,可以使研究结果更科学,更严密,更深刻。本文主要针对评估 IT 风险的有效性和符合性问题,基于绝对损失效应及相对损失效应的概念,在此基础上建立了基于效用的 IT 风险度量模型。该模型克服了常用期望损失理论的弱点 不能比较高损失、低概率与低损失、高概率风险事件间的差异,以及不同规模组织对同样损失的风险承受能力的差异。在度量风险时,将绝对损失效应和相对损失效应联合起来一起分析,提高了风险评估的确定性、符合性和有效性。

参考文献

1 Kevin J, Soo H. a risk – management approach to computer security. School of Engineering, Stanford University,2000.

2 赵战生. 信息安全风险评估. 中国科学院研究生院信息安全国家重点实验室,2004.

3 韩权印,张玉清,王阂,聂晓伟. 信息安全管理实施要点研究. 计算机工程,2005,(10):64 – 66.

4 刘伟,张玉清,冯登国. 信息系统安全风险模型一 RC 模型. 计算机工程与应用,2005,(7):122 – 124.