一种改进风险矩阵法在网络系统风险评估中的应用①

付　沙

(湖南财政经济学院 信息管理系，长沙 410205)

摘　要：基于对某高校校园网络系统风险及其影响因素的分析，运用改进的风险矩阵法对校园网络系统七大风险要素进行评价，并构建了应用于校园网络系统风险评估的风险矩阵，设计了利用风险矩阵进行风险评估的基本流程，以期为该高校校园网络系统的风险评估提供一种科学、合理且有效的评估方法。通过实例应用表明该方法的计算结果相对传统方法更加合理，评价更为客观。

关键词：风险矩阵；网络系统；风险评估；Borda 序值；风险地图

Application of an Improved Risk Matrix Method to Network System Risk Assessment

FU Sha

(Department of Information Management, Hunan University of Finance and Economics, Changsha 410205, China)

Abstract: Based on the analysis of the campus network system risk and its impact factors of a university, we evaluated seven major risk factors of campus network systems with the improved risk matrix method, and built the risk matrix used in the risk assessment of campus network system, designed the basic procedure of the risk assessment with the risk matrix, in order to provide a scientific, reasonable and effective evaluation method to the risk assessment of this campus network systems. An example application shows the result of this method is more reasonable and the evaluation is more objective compared to traditional methods.

Key words: risk matrix; network system; risk assessment; Borda count; risk map

随着计算机技术与网络通信技术的飞速发展，各高校纷纷构建校园网络系统，给校内信息资源共享带来了便捷，并提高了学校的教学、科研质量和管理效率，但同时也面临着日益严重的网络安全问题。校园网络系统的风险评估已受到各高校管理者和网络技术人员的高度重视，并成为网络与信息安全领域内一个重要的研究课题[1]。目前，国内外关于风险评估方法的研究大多集中在层次分析法、模糊综合评价法和神经网络等应用，这些方法主要是根据风险发生后的影响程度确定项目的风险等级，没有充分考虑风险发生的概率，易导致评估结果与实际情况有较大差距。项目风险应综合考虑风险影响和风险概率两方面因素。

1　构建应用于校园网络系统风险评估的风险矩阵

风险矩阵法由美国空军电子系统中心（ESC，Electronic Systems Center）于 1995 年 4 月提出，是在项目管理过程中识别项目风险重要性的一种结构性方法，能够对项目风险的潜在影响进行评估，是结合了定性与定量分析且操作简便的方法[2]。

根据我国信息安全的相关评估准则，其风险评估基础包含威胁、脆弱性和资产的识别。在国际信息安全管理实践规范 ISO/IEC17799 的基础上，针对高校校园网络系统的现状并结合风险矩阵法的特点，提出了校园网络系统风险矩阵风险评估模型，如图 1 所示。

在上述风险评估模型中，确定风险矩阵是模型的基础，其构建过程如下：

① 风险矩阵栏目的确定

依照提出的风险评估模型，得出可用于校园网络系统风险评估的风险矩阵，具体栏目如表 1 所示。

① 收稿时间:2011-05-12;收到修改稿时间:2011-06-19

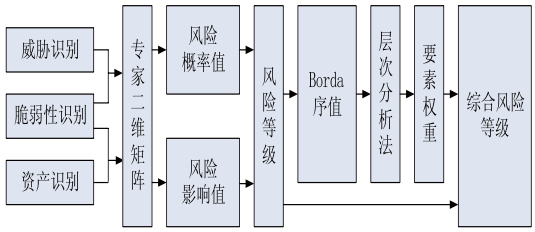

图 1 校园网络系统风险矩阵风险评估模型

表 1 校园网络系统风险矩阵栏目

风险项(R)	风险影响(I)	风险概率(P)	风险等级(RR)	Borda序值

② 风险要素的确定

风险要素的确定可根据该校园网络系统的具体特征、所涉及的技术和所处的规模，在参考有关网络系统风险指标体系研究成果的基础上，总结出校园网络系统七大风险要素，即：硬件设备建设、软件系统建设、校园网络管理、网络教学资源建设、自然灾害与环境干扰、人为攻击或破坏行为、网络应用与服务。

③ 风险概率栏和影响栏的说明

风险概率和风险影响是确定风险等级的基础，根据 GB/T 20984-2007 中的等级划分规则，将风险概率和风险影响各划为 5 个等级[3]，风险影响的等级说明如表 2 所示。确定风险概率和风险影响的基础是威胁、脆弱性和资产的识别，GB/T 20984-2007 将威胁、脆弱性和资产的等级均定义为 5 个等级。

表 2 风险影响的等级说明

影响等级	定义或说明
关键 (5 级)	风险事件将导致整个项目失败
严重 (4 级)	风险事件将导致项目的目标指标严重下降
一般 (3 级)	风险事件将使项目受到中度影响，目标能部分达到
微小 (2 级)	风险事件将使项目受到轻度影响，目标仍能达到
忽略 (1 级)	风险事件对项目基本没有影响

风险概率值 P 由威胁出现频率 T 和脆弱性严重程度 V 来确定：$P = f_1(T,V)$，风险影响值 I 由资产价值 A 和脆弱性严重程度 V 来确定：$I = f_2(A,V)$。f_1、f_2 表示构建专家二维矩阵，矩阵行均代表脆弱性严重程度。f_1 中，列代表威胁出现频率，f_2 中，列代表资产价值；以此行、列建立矩阵，矩阵内的值分别是风险概率值 P 和风险影响值 I。因为不同的脆弱性与不同的威胁或资产价值结合导致的风险概率或风险影响具有随机性，所以矩阵内数值的计算不一定遵循统一的计算公式，计算方法由专家组确定[4,5]。

④ 风险等级栏的确定

通过将风险概率栏和风险影响栏的值代入风险矩阵来确定风险等级，将风险等级划分为“很低、低、中、高、很高”5 档，其具体对照表如表 3 所示。

表 3 风险等级对照表

风险概率	风险影响									
	1 级		2 级		3 级		4 级		5 级	
1 级	0.5	很低	1	很低	1.5	低	2.5	中	3	中
2 级	1	很低	1.5	低	2	低	2.5	中	3.5	高
3 级	1.5	低	1.5	低	3	中	3	中	4	高
4 级	2.5	中	3	中	3	中	3.5	高	4.5	很高
5 级	3	中	3.5	高	4	高	4.5	很高	5	很高

⑤ 风险权重的确定

校园网络系统的风险评估是一个有多项评估指标的系统，能真实地反映各风险要素的重要程度，其指标权重的确定极为关键。对此可应用 Borda 序值法，该方法根据多个评价准则将风险按照重要性进行排序，具体原理为：设 N 为风险矩阵中的风险总个数，i 为某个特定风险，k 表示某一准则。风险矩阵有两个准则：用 k= 1 表示风险影响 I，k= 2 表示风险概率 P0。如果 rik 表示风险 i 在准则 k 下的风险等级，则风险 i 的 Borda 数可由下式给出：$b_i = \sum_{k=1}^{n}(N - r_{ik})$

将 Borda 数按从大到小的顺序排列可得出 Borda 序值，用来表示风险的重要程度[6]。依据 Borda 序值法将风险要素按重要性排序后，通过邀请专家组针对校园网络系统的七大风险要素进行两两比较判断以构

建判断矩阵，再利用层次分析法确定校园网络系统各风险要素的权重。

⑥ 综合风险等级的确定

常用的评级方法采用加权法，将各风险要素的风险等级量化值 RRi 与相对应的风险权重 RWi 相乘，然后将得到的结果累加，即可得到该校园网络系统的综合风险等级量化值 RRT，则有：$RRT=\sum_{i=1}^{k}RR_i\times RW_i$

2 实例应用

根据校园网络系统的现状，构建出该高校校园网络系统的结构图如图 2 所示。

① 依据专家的判断及其经验，对其风险概率和风险影响做出评估，并构建二维矩阵，即 f1、f2 遵循[7]：

$f_1=\alpha t+\beta v$

其中，$\alpha=\begin{cases}1, & t\le 2\\ 2, & 2<t\le 5\end{cases}$，$\beta=\begin{cases}2, & v\le 2\\ 3, & 2<v\le 5\end{cases}$

$f_2=\phi a+\varphi v$

其中 $\phi=\begin{cases}2, & a\le 3\\ 3, & 3<a\le 5\end{cases}$，$\varphi=\begin{cases}1, & v\le 3\\ 2.5, & 3<v\le 5\end{cases}$

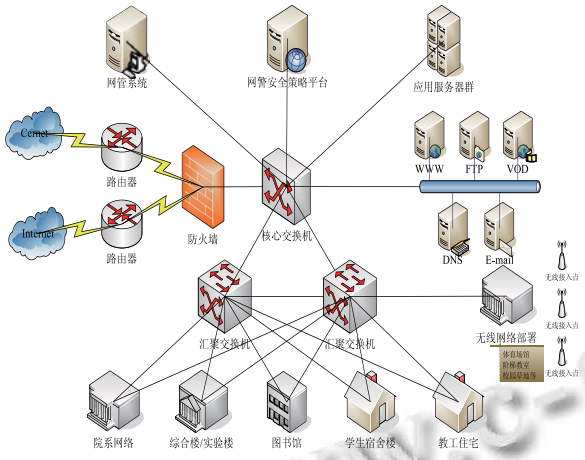

图 2 校园网络系统的结构图

将二维矩阵表格化，如表 4、表 5 所示。

表 4 二维矩阵法求出风险概率值

P=f1(t,v)		脆弱性识别 (v)				
		1	2	3	4	5
威胁识别 (t)	1	3	5	10	13	16
	2	4	6	11	14	17
	3	8	10	15	18	21
	4	10	12	17	20	23
	5	12	14	19	22	25

表 5 二维矩阵法求出风险影响值

I=f2(a,v)		脆弱性识别 (v)				
		1	2	3	4	5
资产识别 (a)	1	3	4	5	12	14.5
	2	5	6	7	14	16.5
	3	7	8	9	16	18.5
	4	13	14	15	22	24.5
	5	16	17	18	25	27.5

以七大风险要素之一“硬件设备建设”为例，其脆弱性识别等级为 3，威胁识别等级为 5，资产识别等级为 4，查表 4 和表 5，确定“硬件设备建设”的风险概率值为 19，风险影响值为 15。

② 根据上述专家二维矩阵评估标准，专家组生成具有针对性的风险概率和风险影响的等级划分表，如表 6、表 7 所示。

表 6 风险概率等级划分

风险概率值 (P)	1 – 5	6 – 11	12 – 16	17 – 21	22 – 25
风险概率等级	1	2	3	4	5

表 7 风险影响等级划分

风险影响值 (I)	1 – 5.5	6 – 12	12.5 – 17.5	18 – 23	23.5 – 27.5
风险影响等级	1	2	3	4	5

“硬件设备建设”的风险概率属于第 4 等级，风险概率为：

$$\Gamma=\frac{\text{风险发生概率值}}{\text{风险概率的最大值}}=\frac{19}{25}=76\%$$

风险影响属于第 3 等级。

③ 将“硬件设备建设”的风险概率等级和风险影响等级代入表 3，可得其最终风险等级量化值为 3，属中等级别。同理，可得校园网络系统其它六个风险要素的风险概率和风险影响等级。结合实际评估确定应用于校园网络系统风险评估的风险矩阵，如表 8 所示。

表 8 应用于校园网络系统风险评估的风险矩阵

编号	风险项(R)	风险影响 (I)	风险概率 (P)		风险等级 (RR)	
			等级	量化值	等级	量化值
①	硬件设备建设	3	4	76%	中	3
②	软件系统建设	4	3	56%	中	3
③	校园网络管理	1	2	24%	很低	1
④	网络教学资源建设	2	4	68%	中	3
⑤	自然灾害与环境干扰	3	2	32%	低	2
⑥	人为攻击或破坏行为	3	3	48%	中	3
⑦	网络应用与服务	1	1	12%	很低	0.5

④ 以“硬件设备建设”为例，根据风险影响准则，比其影响程度高的要素个数为 1，即 r_{11}=1；根据风险概率准则，比其发生概率大的要素个数为 0，即 r_{12}=0；代入公式可得，“硬件设备建设”的 Borda 数为：

$$b_1=\sum_{k=1}^{2}(N-r_{ik})=(7-1)+(7-0)=13$$

同理，可求出其余 6 个风险要素的 Borda 数分别为：12、5、10、9、11、3。根据其 Borda 数可以确定其 Borda 序值分别为：0、1、5、3、4、2、6。

⑤ 进行评判的专家组成员共有 11 人，其成员均长期从事网络与信息安全研究，专业知识丰富，思维和判断能力较强，能够通过不同的角度提供较为全面的意见。

根据得出的 Borda 序值，邀请专家组对该校园网络系统的七个风险要素按重要性程度进行两两比较判断，并构建判断矩阵。每位专家给出一个判断矩阵，然后通过对多个判断矩阵中的相应的元素求取简单算术平均值，得到最后的综合判断矩阵，并做一致性检验[8]。综合判断矩阵为 A：

$$A=(a_{ij})_{7\times7}=\begin{bmatrix}1&1/2&1/6&1/4&1/5&1/3&1/7\\2&1&1/5&1/3&1/4&1/2&1/5\\6&5&1&3&2&3&1/2\\4&3&1/3&1&1/2&2&1/4\\5&4&1/2&2&1&3&1/3\\3&2&1/3&1/2&1/3&1&1/4\\7&5&2&4&3&4&1\end{bmatrix}$$

⑥ 利用求根法确定各风险要素的权重，其运算过程如表 9 所示。

$$CI=\frac{\lambda_{\max}-n}{n-1}=\frac{7.2146-7}{7-1}=0.0358$$

通过查询随机一致性指标 RI 的数值表可得：$RI=1.32$

$$CR=\frac{CI}{RI}=\frac{0.0358}{1.32}=0.027<0.1$$

表 9 应用求根法确定各风险要素权重的计算表

按行相乘	开 7 次方	权重 (RW_i)	$A\cdot RW_i$	$A\cdot RW_i/RW_i$
0.000198	0.295857	0.0315	0.227334	7.216939
0.003333	0.442716	0.0472	0.33924	7.187288
270	2.225039	0.2370	1.70225	7.182489
1	1	0.1065	0.769125	7.221831
20	1.534127	0.1634	1.178533	7.212566
0.083333	0.701183	0.0747	0.535242	7.165216
3360	3.189795	0.3397	2.4852	7.315866
				$\lambda_{\max}=7.2146$

因此，该判断矩阵具有满意的一致性。校园网络系统七大风险要素的权重为：

$$RW=(0.031,0.047,0.237,0.107,0.163,0.075,0.34)$$

⑦ 依据公式得出最后该高校校园网络系统的综合风险等级：

$$RRT=\sum_{i=1}^{7}RR_i\times RW_i=3\times0.031+3\times0.047+1\times0.237+3\times0.107+2\times0.163+3\times0.075+0.5\times0.34=1.5134\approx2$$

根据结果，判断该校园网络系统的综合风险等级为低风险。所列系统各风险要素中，硬件设备建设、软件系统建设、网络教学资源建设、人为攻击或破坏行为四项要素的风险等级量化值为 3，高于系统的综合风险等级，应予以重点关注并采取相应的优先措施以防范上述风险要素带来的损失。

3 利用风险地图进行风险分类评价

为了对该校园网络系统风险发生的可能性和后果严重程度进行二维分析，使风险更为直观地显现，可绘制相应的风险二维图，如图 3 所示。将表 8 中的七个风险要素归类到各个象限中，不仅能帮助管理者找出需要优先处理的风险，以便其做出决策，同时促使管理者针对风险的不同属性采用更合理的管理方法。

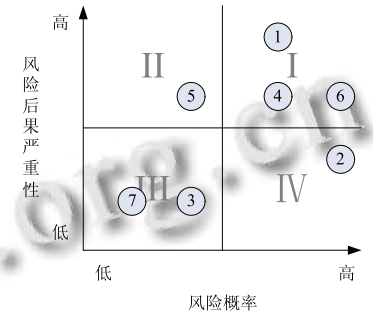

图 3 高校校园网络系统风险二维图

(1) 象限Ⅰ中的风险要素是最需要管理者注意的，硬件设备建设、网络教学资源建设、人为攻击或破坏行为这三项风险要素不仅发生概率高而且后果严重，这些是校园网络系统的核心风险，是风险管理工作的重点，应采取有效措施减少其发生的可能性或降低后果的严重性。

(2) 象限Ⅱ中的风险要素发生的频率低但后果却严重，如自然灾害和环境干扰就归类于这个象限。这类风险因为后果严重，应事先采取一定的预防措施。

(下转第 167 页)

行了仿真，结果表明,利用该算法整定的 PID 控制器调整时间短，响应速度快，超调小，系统鲁棒性较强。总之，该算法具有较高的实用价值和现实意义。

参考文献

1 刘娇.改进 PSO 算法在主汽温系统 PID 参数优化中的应用.计算机与现代化,2009,12:29–32.

2 金翠云等.改进的 PSO 算法及其在 PID 控制器参数整定中的应用.电子测量与仪器学报,2010,24(2):141–146.

3 邵会峰.改进粒子群算法在 PID 参数整定中的应用.电气传动自动化,2010,32(2):22–24.

4 邓伟林,胡桂武.粒子群算法研究与展望.现代计算机(专业版),2006,(11):12–15.

5 徐春梅,等.火电厂主汽温控制系统的自抗扰控制仿真研究.华北电力大学学报,2006,33(3):4145.

6 Arumugam Senthil M, Rao MVC On the Improved Performances of the Particle Swarm Optimization algorithms with Adaptive Parameters, Crosmover Operators and Root Mean Square (RMS) Variants for Computing Optimal Co–ntrol of a Class of Hybrid Systems. Applied Soft Computing, 2007, (2):324–336.

7 龚纯等.精通 PID 最优化计算.北京:电子工业出版社,2009.

8 韩璞,等.控制系统数字仿真技术.北京:中国电力出版社,2008.

9 任子武,等.改进 PSO 算法及在 PID 参数整定中应用研究.系统仿真学报,2006:2870–2873.

10 吕振肃,候志荣,等.自适应变异的粒子群优化算法.电子学报,2004,32(3):416–420.

11 王伟,张晶涛,柴天佑.PID 参数先进整定方法综述.自动化学报,2000,26(3):347–355.

12 王凌,李文峰.非最小相位系统控制器的优化设计.自动纪学报,2003,29(1):135–141.

13 陶永华.新型 PID 控制及其应用.北京:机械工业出版社,2003.

14 谢晓锋,张文俊,杨之廉.微粒群算法综述.控制与决策,2003,18(2):129–134.

(上接第 151 页)

(3) 象限Ⅲ中的风险发生的可能性和严重性都较低，如校园网络管理、网络应用与服务等，通常这类风险不需要立即采取措施应对，但需要定期的监控以确定该类风险是否已经转化为其它象限的风险。

(4) 象限Ⅳ中的风险发生频率高，但后果并不严重，如软件系统建设，这类风险通常可以通过改进管理方法或采取一些控制手段来降低其发生频率。

4 结语

本文对一种改进的风险矩阵法在校园网络系统风险评估中的应用进行了探讨，研究结果表明运用风险矩阵法对校园网络系统的评估从风险影响程度和风险概率两个维度来进行，克服了层次分析法等评估方法仅从单方面评估的缺点。该方法较好地综合了群体的意见，增加了评估结果的客观性，而受到越来越更广泛的重视。

参考文献

1 付沙.高校校园网信息安全策略的探索.中国教育信息化,2008,(1):63–65.

2 陈志敏.高技术计划项目的风险评价体系.西安交通大学学报(社会科学版),2008,28(3):49–52.

3 熊杰,张善从.基于 AHP 和风险矩阵的航天研制项目风险评估.科技进步与对策,2010,27(11):124–126.

4 孙强.信息安全风险评估模型的定性与定量对比研究.微电子学与计算机,2010,27(6):92–96.

5 付钰,吴晓平,叶清,彭熙.基于模糊集与熵权理论的信息系统安全风险评估研究.电子学报,2010,38(7):1489–1494.

6 李聪波,刘飞,谭显春,李彩贞.基于风险矩阵和模糊集的绿色制造实施风险评估方法.计算机集成制造系统,2010,16(1):209–214.

7 张弢,慕德俊,任帅,姚磊.一种基于风险矩阵法的信息安全风险评估模型.计算机工程与应用,2010,46(5):93–95.

8 党兴华,黄正超,赵巧艳.基于风险矩阵的风险投资项目风险评估.科技进步与对策,2006,(1):140–143.