doi:10.3969/j.issn.1000-436x.2012.z1.027

基于业务流程的 ERP 信息安全进化熵的风险评估

宋彪[1,2]，朱建明[1]
（1. 中央财经大学 信息学院，北京 100081；2. 内蒙古财经大学 会计学院，内蒙古 呼和浩特 010051）

摘 要：ERP 内部安全漏洞与业务流程紧密结合，与业务流程呈现共生性，使信息资产的价值具有了动态属性并难以确定，因此此类安全问题不易被及时捕捉和评估。通过对 ERP 系统与其他信息系统在信息安全方面的区别，提出基于业务流程的 ERP 系统信息安全进化熵的概念，并建立了适应 ERP 系统特点的风险评估模型，为 ERP 系统的信息安全风险评估提出了新的思路。

关键词：业务流程；ERP；信息安全；熵；风险评估
中图分类号：TN918.91 **文献标识码**：B **文章编号**：1000-436X(2012)Z1-0210-06

Evolution entropy risk assessment of ERP information security based on the business process

SONG Biao[1,2], ZHU Jian-ming[1]
(1. School of Information, Central University of Finance and Economics, Beijing 100081, China;
2. School of Account, Inner Mongolia University of Finance and Economics, Huhhot 010051, China)

Abstract: ERP internal security holes often bind with business process closely, make the value of information assets has dynamic properties and difficult to determined, so such security will not be prompt capture and evaluation. Compored the difference of ERP system and other information system in the information security, the risk assessment model which adapt to the characteristics of ERP system was proposed, and gave a new idea for the ERP system information safety risk assessment.

Key words: business process; ERP; information security; entropy; risk assessment

1 引言

ERP（enterprise resource planning，企业资源计划）由美国 Gartner Group 公司在 20 世纪 90 年代提出以来，ERP 在国外获得了广泛应用和飞速发展，投资年均增长速度超过 30%，同时也取得巨大的经济和社会效益。在我国，ERP 的发展已有 20 多年，《2009~2010 中国 IT 应用技术蓝皮书》中显示，目前 50.7%的企业拥有 ERP 系统，同时还有大量企业筹备或正在实施 ERP 项目。

由于 ERP 系统项目的投资大，软件涉及的业务流程复杂，因此企业在实施项目时往往只关注投资的收益和业务流程的实现，而忽略 ERP 系统的信息安全。ERP 系统集成了企业所有的相关信息，包括客户信息、BOM 结构、账户情况等，这些信息对别有用心者都具有极大的吸引力。因此，利用 ERP

收稿日期：2012-07-01
基金项目：国家自然科学基金资助项目（60970143）；教育部科学技术研究重点项目基金资助项目（109016）；中央财经大学科研创新团队支持计划基金资助项目；内蒙古自然科学基金资助项目（200508010805）
Foundation Items: The National Natural Science Foundation of China (60970143); Ministry of Education Key Project of Science and Technology (109016); Central University of Finance and Economics Research and Innovation Team Supports Project Grant; The Natural Science Foundation of Inner Mongolia (200508010805)

进行犯罪的事件时有发生，例如上海发生的一家大型跨国连锁超市营业款被窃案为企业敲响了警钟，以收银员、计算机管理员为主的普通员工居然利用超市 ERP 系统的漏洞在短短半年之间悄无声息地从超市窃走 372 万元的营业款。国内某银行在对即将上线的信息系统进行测试时，误将带有蠕虫病毒的主机接入生产系统，造成其生产系统的长时间故障，造成大量经济损失。中国银联信息系统设备曾出现通信网络和主机出现故障，造成辖内跨行交易全部中断，故障时间长达 8 小时，给人们的生活带来了极大的不便。英国保险巨头英杰华集团(Aviva)于 2009 年证实，ERP 系统中的一台机器感染病毒，造成敏感个人信息泄露，估计大约有 550 名保险客户的数据记录被泄露，其中包含用户的姓名、地址和社会安全号码等信息。荷兰银行发生系统中客户资料泄露，巨额存款被黑客盗取事件，涉及金额达 2 000 万人民币。由这些案例可以看出，对 ERP 系统的安全评估进行研究有着重要的现实意义。

2　研究综述

迄今为止，专门关于 ERP 的信息安全风险评估的研究成果不多。一般学术研究都针对 ERP 系统的项目实施风险和 ERP 系统的绩效评估等。朱岩在 2006 年提出 ERP 风险因素的评估方法——“企业资源规划功能配置法（EFD）”[1]。许振宇等在 2006 年提出一个利用风险矩阵和模糊综合评判方法来评估企业实施 ERP 项目风险等级的模型，并利用实例作为研究该评估方法的样本[2]。王立彦等人在 2007 年分析了 ERP 系统的实施和企业绩效增长的关系[3]。在 ERP 系统信息安全方面，陈运明等人在 2009 年提出了一个 PERIVOR 模型，该模型采用动态网络模型和基于策略的网络安全以及风险权值分析技术，通过将各种威胁、脆弱性等风险因素的分级和分类，尽量全面客观地对信息安全的技术性和非技术性以及定性和定量相结合的方式来展示信息安全风险。沈沉等人在 2005 年提出了要引入国外的不间断监控法加强 ERP 系统的安全控制[4]。唐志宏等人在 2003 年指出 ERP 软件极少能够达到第三级安全标准，并针对权限问题给出了一系列改进措施。Wouter Janssen 在 1998 年认为应该把安全问题从数据库级提升至 ERP 级，而且有必要开发更为合适的能够确保安全的工作流管理技术[5]。程乃伟在 2010 年提出了根据 ERP 系统组成的网络拓扑结构，构建链路域的概念，通过确定资产间的影响系数，计算整个链路上的风险[6]。

相对于信息安全评估的领域，则有大量的文献提出了丰富的风险评估方法。主要分定性和定量的 2 类，使用到的定性方法有：头脑风暴法、名义小组评述法(NGT)、德尔菲方法、层次分析法等。定量的对风险进行评估的方法有：统计学模型、成本因素法、CPN 方法、决策树法、故障树的方法、影响图法、人工神经网络的方法、基于规则的系统、灵敏性分析法、Monte Carlo 模拟法、ID3 算法以及 LA-LEARN 算法等[2]。

总之，关于信息系统的安全评估的研究比较成熟，针对 ERP 系统项目实施风险的研究也相对很深入，而 ERP 系统的信息安全方面，一般都是定性的给出一些增强安全系数的方法和措施，只有陈运明在 2009 年提出了一个 ERP 系统安全评估模型，认识到应该把 ERP 系统的安全评估和其他信息系统的安全评估区别开来，其不足之处是没有能够指出深入挖掘出 ERP 系统的信息安全特点，以及进一步给出完全适合于 ERP 特点的评估模型，使评估结果没有针对具体的业务流程，导致无法对企业针对业务流程进行信息安全措施进行改进。而程乃伟在 2010 年的研究把 ERP 的流程节点简单化为网络拓扑节点，同时对信息资产的节点风险以及被影响节点风险简单加和，忽略了信息资产在 ERP 系统中价值变化的高频性。

3　ERP 与一般信息系统的区别

ERP 与一般的信息系统的区别主要体现在以下 6 个方面。

1) ERP 系统的信息资料更加集中，对攻击者更有吸引力。ERP 系统作为数据库平台上的捆绑组件，往往包含着多个其他应用程序的接口，它的特点是信息高度集成和即时共享，系统中运行着许多敏感的业务信息，使用者可以从中寻找出一个企业的组织架构、管理理念、客户资源、财务信息、人力资源组成、企业产能、产品配方、销售渠道、合作伙伴、竞争对手等方方面面的信息。

2) ERP 系统安全问题相对其他信息系统更为复杂。ERP 系统流程涉及范围广，各节点关系紧密，对信息的准确性和及时性要求苛刻，信息集成度越高的 ERP 系统越是如此（企业恰恰追求集成度高的 ERP 系统来提高经济效益），所以在企业中，ERP 系

统一般在其信息系统中居于核心地位，企业对 ERP 系统的依赖性一般要远强于其他信息系统。如果系统遭受攻击，甚至是使系统稍有延迟，都将会对业务流程及生产方面乃至整个企业造成巨大破坏。

3) ERP 系统涉及企业生产业务过程，涉及企业核心业务。攻击者对 ERP 系统攻击的目标更为明确，ERP 系统安全事件的发生以资产为基础，以对系统资产的窃取、攻击和破坏为目标[6]。

4) ERP 系统的信息资产价值不易确定。在传统的信息安全风险评估中得到的往往是以资产为基础的单一风险值。对于 ERP 系统来说，各资产之间是通过各种不同方式和链路连接在一起的，因此，各点的风险因其连接方式的不同，会传递给与之相邻的资产。因此，确定风险的传递方式及整个物理链路上的综合风险就显得尤为重要[6]。ERP 系统的安全漏洞会随着业务流程的流转惯性而逐级放大由该漏洞造成的影响，同一信息资产的价值由于会随着业务节点的不同而发生价值变动，更为重要的一点是，这些价值变动会随着企业的日常业务周而复始的发生，其变动频率会非常高，虽然能确定在哪一节点有安全漏洞，也能确定在该节点时信息资产的价值，但无法确定当该节点安全漏洞发生作用时，影响的后果是否还是该节点时的信息资产的价值，对 ERP 系统依赖程度高的企业愈发如此。因此，对信息资产进行赋值从而进行评估的方法并不适用于 ERP 系统。

5) ERP 系统的业务流程复杂。ERP 系统中存在大量基于业务流程产生的信息安全漏洞，区别于简单的软件中的代码漏洞。一般 ERP 系统的安全问题体现在 3 个方面，网络层、表现层和应用层，而应用层中包括业务流程[7]。ERP 业务流程的复杂性，导致企业更加关注业务的实现，而忽略了信息安全的防范，恰恰现实的情况是，有些安全漏洞在数据静止的情况下评估是无法发现的，而放到不同的业务流程中，这些安全漏洞的评估结果也不相同，这决定了 ERP 系统的信息安全评估不能简单的依靠网络拓扑分解来实现。

6) ERP 系统在生命周期中基于技术进步的进化特征性更强。ERP 系统在整个生命周期内，由于科学技术的不断发展，企业业务规模等情况的变化，以及企业对系统的持续调整都会使信息安全问题呈动态进化趋势，因此其安全评估不能简单截取其某个阶段独立分析，必须着眼于整个生命周期进行分析才可以得出比较客观有意义的评估结果。

4 基于业务流程的 ERP 信息安全进化熵的风险评估

在物理学中，熵是指热力学系统的某种状态函数，它是对系统紊乱程度的度量。玻尔兹曼在 1872 年从气体分子运动的角度得出统计物理学热力学熵 S 的表达式：$s=k\ln w$ 其中，k 是玻尔兹曼常数，W 为系统宏观状态所包含的微观状态数。熵 S 就是系统内部分子运动混乱程度的度量。

美国数学家香农将热力学熵引入信息论，提出了信息熵的概念。在信息论中，信息是系统有序程度的一个度量，而熵是系统无序程度的—个度量。二者绝对值相等，但符号相反。—个系统 X 的信息量大小 H(即信息熵)与该系统的状态概率 p 紧密联系在一起，且概率 p 越小，系统所包含的信息熵 H 越大，而系统信息熵与系统 X 的状态具体取值没有关系。若—个信息系统 X 由状态集$\{a_1,a_2,\cdots,a_n\}$组成，每个状态对应的概率分别为 $p_1,p_2,\cdots,p_n$，且 $\sum_{i=1}^{n} p_i=1$，则系统 X 的信息熵 H 定义为

$$H(x)=H(p_1,p_2,\cdots,p_n)=-k\sum_{i=1}^{m} p_i\log p_i$$

其中，系数 k 取决于度量单位，k 为非负数。最大信息熵原理从理论上说明，假设 k=1，在信息熵取极大值时，对应的一组状态出现的概率占有绝对优势,且上式最大值为 $\log n$。

4.1 基于业务流程的 ERP 信息安全进化熵的风险评估模型

定义 基于业务流程的 ERP 系统信息安全进化熵是指在 ERP 系统在其整个生命周期内进化的过程中，各业务流程节点对应的安全属性对 ERP 系统安全状态的不确定性、混乱性和无序性影响的度量。

$$s_{i,t}=\sum_{j=1}^{n} p_{t-1}j(1+r)^{t-1}\ln p_{t-1}j(1+r)^{t-1}$$

$$(i=1,2,\cdots,m \quad j=1,2,\cdots,n) \tag{1}$$

其中，T 为 ERP 系统生命周期长度，用时栅划分为若干个区间，各时栅为 $t=1,2,\cdots,T$；F 表示系统中业务流程个数；m 表示任一流程包含的节点个数；n 表示任一节点的信息安全确定性属性个数；r 表示在各时栅内对该节点信息安全确定性属性期望安全技术进步系数(可为负值，表示入侵技术的进步大于安全技术的进步)；s 表示某个流程任一节点某时栅的信息安全进化熵；p_{ij} 表示 i 节点在时栅 t 区间 j 信息安全

属性的确认度；式(1)中，$\sum p_{tj}=1, p_{tj}(1+r)^t$，越大，$s$ 值越小，当 $p_{t1}=p_{t2}=\cdots=p_{tj}$ 时，s 值最大，s 值越小表示在某一时栅内，该业务节点对应的信息安全属性相关信息越确定（确定性代表对该节点的安全性认识足够，知道症结所在，能够采取有效措施），该节点处安全性越高，系统亦越安全。对式(1)进行归一化处理得

$$s_{i,t}=\frac{1}{(1+r)^{t-1}(\ln n-\ln(1+r)^{r-1})}\cdot \sum_{j=1}^{n} p_{t-1,j}(1+r)^{t-1}\ln p_{t-1,j}(1+r)^{t-1}$$

$$(i=1,2,\cdots,m \quad j=1,2,\cdots,n) \tag{2}$$

其中，参数涵义同式(1)。计算单个节点的安全属性熵值,概率评估当期 t 值为 1，非当期 t 值根据预测期时栅值减去概率评估期时栅值，p 值是专家评估时选择各节点的安全属性的概率统计，如果各安全属性被选中的概率越接近，说明专家越不确定哪个安全属性为影响安全关键因素，则系统该节点越不安全。

$$e_t=1-s_t \tag{3}$$

其中，e_t 表示某一个流程某一个节点的系统安全性。

式(3)中，e_t 越小表示系统安全性越差。一个流程里面包含 m 个节点，根据 TOC 理论，整个业务流程的安全系数可定义为

$$S_{ht}=[\Pi_1^m e_{i,t}\min(e_{i,t})]^{1/m} \quad h=1,2,\cdots,F \tag{4}$$

其中，$S_{h,t}$ 表示某个流程在 t 时栅的安全性系数。

式(4)突出该业务流程中安全性最差的节点的影响，并以此分析系统安全短板，进行安全措施决策。

$$D=\sum_{ht}^{F} S_{ht}-\frac{Akt}{\sum_{k=1}^{F} A_{kt}} \tag{5}$$

其中，A_{ht} 表示 h 流程在 t 时栅的平均信息资产价值，A_{ht} 值由专家进行评估；D 表示整个 ERP 系统信息安全进化熵系数。

$$I\leqslant A_{ht'}S_{ht'}-A_{ht}S_{ht} \tag{6}$$

其中，I 为投资金额；式(6)可用来进行安全投资决策，即投资要小于安全收益。

4.2　风险评估算法

算法 1　基于业务流程的 ERP 信息安全进化熵的风险评估算法

输入：($p[m,n]$,$m[h]$,$n[k]$,F,$a[h]$,t,r)

输出：系统信息安全进化熵系数 D

1) 由专家初始化输入集($p[m,n]$,$m[h]$, $n[k]$, F, $a[h]$,t,r)；

2) for all　ERP 系统所有节点安全确定性属性 do；

3) 计算各个节点信息安全进化熵 S；

4) for all 各个流程的所有节点 do；

5) 计算各个流程信息安全进化熵 $S_{h,t}$；

6) for all 各个 ERP 系统的流程 do；

7) 计算 ERP 系统的信息安全进化熵系数；

8) return D；

算法 2　ERP 信息安全进化熵公式计算求解具体算法

输入：($p[m,n]$,$m[h]$,$n[k]$,F,$a[h]$,t,r)

输出：系统信息安全进化熵系数 D

//输入参照时栅某个流程某个安全节点安全属性的确定性概率,业务流程个数、各业务流程节点个数、对应各节点安全属性个数、各流程信息资产价值、时栅值、技术进步系数。

//输出系统信息安全进化熵

1) for $h\leftarrow$1 to F do
2) $A\leftarrow A+a[h]$
3) for $h\leftarrow$1 to F do
4) $B[h]\leftarrow a[h]/A$
5) for $h\leftarrow$1 to F
6) $f\leftarrow$1
7) for $k\leftarrow$1 to $m[h]$ do
8) for $j\leftarrow$1 to $n[k]$ do
9) if t=1
10) $v\leftarrow v+p[k,j]*\ln p[k,j]$
11) else $v\leftarrow v+p[k,j]*(1+r)^{t-1}*\ln p[k,j](1+r)^{t-1}$
12) $z[k]\leftarrow 1-\frac{1}{\ln n} * v$
13) $f\leftarrow f*z[k]$
14) min $z\leftarrow z[1]$
15) for $i\leftarrow m[h]-1$
16) if $z[i]<\min z$
17) min $z\leftarrow z$
18) $f\leftarrow(f*\min z)^{1/m}$
19) $g[h]\leftarrow f$
20) for $h\leftarrow$1 to F
21) $D\leftarrow s+g[h]*B[h]$
22) return D

4.3 评估模型仿真

假设将某企业 ERP 系统在其生命周期内用时栅划分为 4 个阶段（可以更为细致的划分），而流程有采购、销售、仓储，为了简化模拟，假设只有这 3 个流程。设采购有 4 个信息安全节点，销售有 4 个安全节点，仓储有 4 个安全节点，生产流程有 4 个安全节点，假设采购流程的 4 个信息安全节点的确定性属性个数都为 5，销售流程的 4 个信息安全节点的确定性属性个数都为 5，仓储流程 4 个信息安全节点的确定性属性个数都为 3，生产流程的 4 个信息安全节点的确定性属性个数都为 4，时栅间隔内利率没有变化，如表 1 所示。

表 1　　ERP 状态划分情况

时栅划分	流程	安全属性	平均信息资产价值
设计阶段	采购	采购 5 个	A
开发阶段	销售	销售 5 个	
实施阶段	仓储	仓储 3 个	
运营维护阶段	生产	生产 4 个	

用 SaaS 软件模拟安全属性确定性随机概率(开发阶段)。

安全属性每个不确定性为 0~1 之间，本仿真用 sas 软件随机概率模拟专家们对逐个对节点各安全属性做出的选择，统计该节点各安全属性被选中的概率，如表 2 所示。

表 2　　节点属性确定概率

流程	P1	P2	P3	P4	P5
采购组	0.250 052	0.196 688	0.108 217	0.158 255	0.286 787
	0.193 929	0.321 049	0.139 709	0.210 965	0.134 348
	0.387 155	0.237 914	0.028 562	0.034 926	0.311 442
	0.245 609	0.055 693	0.280 211	0.179 219	0.239 269
销售组	0.065 007	0.313 882	0.137 697	0.339 315	0.144 099
	0.355 44	0.055 739	0.268 415	0.028 391	0.292 016
	0.055 908	0.157 965	0.273 899	0.259 961	0.252 267
	0.028 647	0.298 682	0.138 905	0.343 35	0.190 415
仓储组	0.266 615	0.642 363	0.091 022		
	0.220 413	0.651 043	0.128 544		
	0.322 757	0.326 537	0.350 707		
	0.146 003	0.284 153	0.569 844		
生产组	0.397 186	0.388 863	0.209 785	0.004 167	
	0.161 086	0.284 135	0.401 891	0.152 888	
	0.245 728	0.427 192	0.036 018	0.291 063	
	0.328 882	0.199 842	0.086 082	0.385 194	

开发阶段：

由式(2)可计算，

采购 S1=0.967 43　　S2=0.966 665
　　S3=0.802 156　　S4=0.939 744
销售 S1=0.907 344　　S2=0.833 949
　　S3=0.935 178　　S4=0.882 137
仓储 S1=0.778 173　　S2=0.797 771
　　S3=0.999 377　　S4=0.872 863
生产 S1=0.782 291　　S2=0.941 45
　　S3=0.856 363　　S4=0.913 31

则可由式(4)计算，开发阶段采购流程的安全系数：S 采购= 0.025 480 902　S 销售= 0.052 539
S 仓储= 0.006 859　　S 生产=0.055 213

假设整个信息系统信息资产在采购流程中平均资产价值（指在本阶段如发生安全事件产生的损失）为 100 000 元，在仓储阶段平均价值为 150 000 元，在生产阶段为 120 000 元，在销售阶段为 200 000 元，则由式(5)计算系统整体安全系数为 S=0.394 1。

现假设企业要进行杀毒软件投资，投资额为 5 000 元，期望在运行阶段达到技术进步率为 r=0.2，时栅相差为 1，则可以根据进化熵计算出系统整体安全系数为

运行阶段：

由式(2)可计算，

采购 S1=0.963 27　　S2=0.962 406
　　S3=0.776 88　　S4=0.932 046
销售 S1=0.895 495　　S2=0.812 736
　　S3=0.926 896　　S4=0.867 079
仓储 S1=0.734 034　　S2=0.757 531
　　S3=0.999 253　　S4=0.847 566
生产 S1=0.749 322　　S2=0.932 584
　　S3=0.834 611　　S4=0.900 182

则可由式(4)计算运行阶段采购流程的安全系数：S 采购= 0.029 612 732　S 销售= 0.061 061
S 仓储= 0.008 606　　S 生产= 0.065 855

资产价值仍如上假设（实际操作中可以考虑资金时间价值），则由式(5)计算系统整体安全系数为：S=0.461 83。

0.461 83−0.394 1=0.067 33，即系统安全系数提高了 0.067 33，资产价值均值为 142 500，则由式(6)计算投资收益为 9 651 元，则由投资收益分析可知企业应该进行杀毒软件投资。

5　结束语

该评估模型充分考虑了 ERP 系统在安全评估方面的特点，把评估点细分到各业务流程的节点，利用熵的概念把影响各业务节点的安全属性对系统安全的影响予以描述，在模型中体现了 ERP 系统进化的过程对安全的影响，做出生命周期内某一期间的评估后，可以对其他期间进行预测，同时应用 TOC 理论确定了业务流程的安全系数，并根据信息资产权重解决了 ERP 系统中信息资产动态变化导致的评估难题，最终对 ERP 系统计算出了量化的安全评估结果，为 ERP 系统的安全投资决策提供了量化的参考依据。

参考文献：

[1] 朱岩. 一种 ERP 风险评估法——企业资源功能展开法 EFD[J]. 清华大学学报,2006,46(S1): 15-19.
ZHU Y. EFD — a risk assessment method of enterprise resource planning implementation[J]. Tsinghua Science and Technology, 2006, 46(S1): 15-19.

[2] 许振宇. 基于模糊综合评判的 ERP 项目风险评估[J]. 情报杂志, 2006,(8): 89-93.
XU Z Y. Risk assessment of ERP project based on fuzzy synthesis judgment[J]. Journal of Information, 2006,(8): 89-93.

[3] 王立彦. ERP 系统实施与公司业绩增长之关系——基于中国上市公司数据的实证分析[J]. 管理世界, 2007,(3):116-121.
WANG L Y. Relationship of the ERP system implementation and performance of the company growth-empirical analysis based on the data of China's listed companies[J]. Management World, 2007,(3): 116-121.

[4] 沈沉. ERP 安全现状和解决方案[J]. 网络安全技术与应用, 2005,(5): 16-17.
SHEN C. ERP security current situation and solution[J]. Network security technology & application, 2005,(5): 16-17.

[5] MICHAEL E, WHITMAN H J. Principles of Information Security[M]. Canada: GEX Publishing Services, 2003.

[6] 程乃伟. ERP 系统安全风险评估方法研究[A]. 2010(沈阳)国际安全科学与技术学术研讨会论文集[C]. 沈阳, 中国, 2010. 50-53.
CHENG N W. Study on the method of security risk assessment for ERP system[A]. Proceedings of 2010(Shenyang) International Colloquium on Safety Science and Technology[C]. Shenyang, China, 2010. 50-53.

[7] WEI S, THURAISINGHAM B. Security for enterprise resource planning systems[J]. Information Systems Security, 2007. 16(3):152-163.

[8] IFINEDO P. Relationship among ERP post-implementation success constructs:An analysis at the organizational level[J]. Computers in Human Behavior, 2010, 26(5):1136-1148.

[9] HAKIM A. A practical model on controlling the ERP implementation risks[J]. Information Systems, 2010, 35(2):204-214.

[10] 叶强. 组织因素对 ERP 使用绩效的影响机制[J]. 管理科学学报, 2010, 13(11): 77-81.
YE Q. Impact of organizational factors on ERP usage and performance[J]. Journal of Management Sciences in China, 2010, 13(11): 77-81.

作者简介：

宋彪（1983-），男，蒙古族，内蒙古兴安盟人，中央财经大学博士生，内蒙古财经大学讲师，主要研究方向为 ERP 项目实施与开发、数据挖掘、信息安全、网络舆情。

朱建明（1965-），男，山西太原人，中央财经大学信息学院教授、博士生导师、院长，主要研究方向为信息安全、电子商务安全和无线网络安全。