文章编号：1007－5399（2013）06－0017－03

邮政系统信息化风险控制研究

孟 妍

（山东省邮政公司，山东 济南 250014）

摘 要：文章分析了邮政系统信息化过程中存在的各种风险，探讨了风险控制模型 PS－HRCM 的构建及其特点，并提出了风险量化模型的具体计算方法。

关键词：邮政系统；信息化；安全风险；风险控制

中图分类号：F61 **文献标识码**：A

信息技术作为推动社会发展的强有力因素，已成为世界经济增长的重要动力。中国邮政经过百年发展，现已建成覆盖全国较为完善的实物传递网络，而近几年邮政系统信息化的发展也使邮政系统成为连接全国各地的邮政综合计算机网络。如今，信息已经成为不可或缺的战略资源，信息安全和信息安全风险的内涵也随之得到扩充和拓展。只有有效控制邮政系统信息化过程中产生的各种风险，才能满足预期的信息安全目标。

1 信息化过程存在的各种风险

1.1 IT 投入风险

IT 治理体系的设计与实施，企业的未来发展战略、核心文化、组织架构等深层次因素不能达到完美结合，且执行不够有效，致使 IT 技术系统无效或给企业带来负面影响，甚至产生治理体系失效的风险。

1.2 信息系统安全风险

当信息系统发生故障、停止运行或者系统丧失有效功能时，系统影响到的各领域活动都将失去保障，从而带来巨大损失，甚至影响社会的正常运转。

2 邮政系统信息化风险控制模型 PS-HRCM 的构建

为了有效控制邮政系统信息化过程中产生的各种风险，本文有效借鉴国际主流信息技术控制相关标准 COBIT，构建一个多层次、面向信息化全生命周期过程的信息化风险治理结构 PS-HRCM（见图 1），采用包含战略目标层、风险评价控制层、标准参照层的多层次结构，从企业战略、目标导向和主动风险应对等多维视角对邮政企业 IT 治理中的各种风险进行研究，并采取信息系统审计等内部控制机制加强风险的管理和控制，使信息化过程中的风险管理更加充分、有效、全局和客观。

2.1 模型描述

2.1.1 战略目标层

战略目标层通过对企业战略、业务经营、竞争环境和技术发展的分析，确定企业商业目标需求。

2.1.2 风险评价控制层

风险评价控制层处于 PS－HRCM 模型的第二层，它根据战略目标层的指导进行 IT 治理中的风险控制工作，同时也是信息化风险控制审计工作的工作对象。

2.1.3 标准参照层

标准参照层是整个 IT 治理层次风险控制模型有关 IT 治理和风险控制的各种国际标准的集合，主要参照国际信息系统审计与控制协会（ISACA：Information System Audit and Control Association）与 IT 治理研究所（IT Governance Institute）研究与开发的“信息及相关技术的控制目标”（COBIT）。

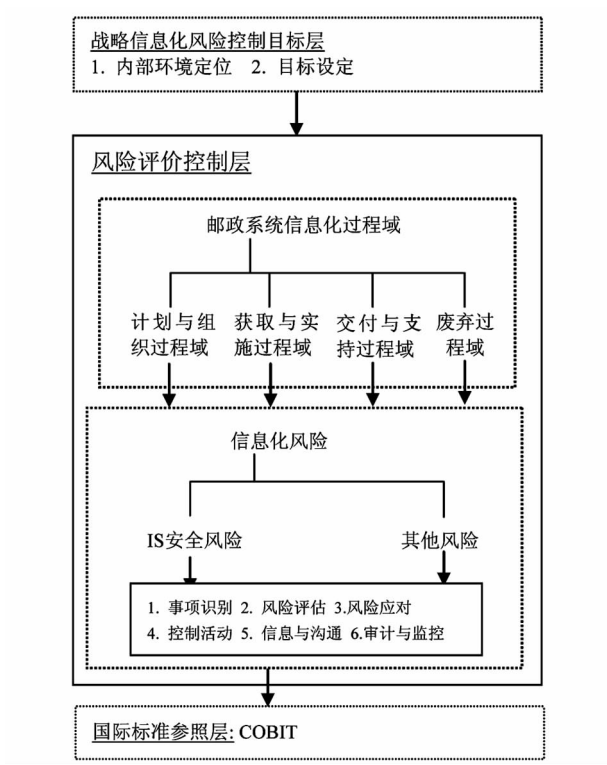

图 1 邮政系统信息化风险控制模型 PS-HRCM

2.2　模型特点

2.2.1　层次化框架架构

PS-HRCM 是一个包含战略目标层、风险评价控制层、标准参照层多层次的 IT 风险控制模型。企业信息化具有多级管理、过程复杂、人员结构和技术难以控制等特点，其 IT 治理过程也比较复杂。组织的体系结构通常采用决策层、管理层和控制层的体系结构进行管理，为了更好地对信息化过程中的各种风险进行管理控制，所以选用层次结构的风险控制模型。

2.2.2　面向全生命周期过程的风险控制

将 IT 治理的整个过程按照信息系统生命周期分为四个过程域，分别是计划与组织过程域、获取与实施过程域、交付与支持过程域和废弃过程域。IT 治理中的风险控制从企业信息化启动阶段开始，采用主动风险应对策略，在启动阶段根据企业战略目标进行风险控制和 IT 审计，将 IT 治理各个阶段的风险降至最小，这也是整个 IT 治理风险控制最重要的环节之一。

3　PS-HRCM 控制模型的风险量化及计算

3.1　Finne 的风险概念模型

目前的信息安全风险评估方法大多继承了 Finne 提出的概念模型的传统思路，即从信息系统漏洞、可能受到的攻击和信息资产损失三方面评估风险及其大小。该模型表示如下式（3－1）。Finne 从技术的观点认为信息安全风险是威胁（T）利用漏洞（V）对信息资产（A）造成损失的可能性及潜在损失的大小。

$$R=F(A,V,T) \qquad (3-1)$$

按照 Yates 和 Stone 提出的风险结构三因素模型的概念框架，即风险包括潜在损失、损失大小和潜在损失发生的不确定性三方面内涵，Finne 的模型是科学、合理的，但在实践上遇到如下问题：信息资产不同于可货币化的实物资产，其估值是个公认的难题，潜在损失较难度量。

信息资产价值具有相对性，即某个机构认为非常重要的信息，对另一个机构而言可能毫无价值。因此，对信息资产简单赋值并以此为依据来评估信息安全风险，其结果未必有说服力。

3.2　ITG-HRCM 的风险量化与计算

在邮政企业信息化过程中，要关注由于各种威胁利用脆弱性导致的风险而给系统带来的损失。

3.2.1　风险要素的量化

为了克服 Finne 概念模型存在的问题，提高 ITG-HRCM 风险量化效果，对风险量化作如下改进。设资产的集合为 A＝｛a_1，a_2，a_3……｝，资产 a∈A 的脆弱性集合为 Va＝｛v_1，v_2，v_3……｝；相应的威胁的集合为 Ta＝｛t_1，t_2，t_3……｝；安全事件的集合为 Ea＝｛e_1，e_2，e_3……｝；安全措施的集合为 Sa＝｛s_1，s_2，s_3……｝；定义资产 A 的风险向量为 RA＝｛＜a_1，v_1，t_1，e_1，s_1＞，＜a_2，v_2，t_2，e_2，s_2＞，＜a_3，v_3，t_3，e_3，s_3＞……｝

3.2.2　计算风险损失

P（t_i）表示在一定的置信度下，类型为 t_i 威胁发生的概率。

C（e_i）表示一个类型为 e_i 的事件引起的最大可能开销，L 表示可能损失的价值。

f_i 表示脆弱性的量，反映该脆弱点可被威胁利用的可能性的大小，其值域为［0，1］，该值为专家通过历史数据得到的经验值。

P（t_i）×f_i 反映了威胁实际发生的可能性。

对于资产 a，定义相应的权重向量 Wa＝｛w_1^a，w_2^a，w_3^a……｝，该值也为专家通过历史数据得到的经验值。

R 表示可能导致的风险值，于是 R 的取值可以如下计算（3－2）：

$$R_i = a_i \times w_i \times \sum_{t_i \in T_a} P(t_i) \times f_i \times \sum_{e_i \in E_a} C(e_i)$$

4　仿真实验

某市邮政企业信息系统分为两部分，出于安全性考虑，采用内外网严格物理隔离的方式运行。外网为门户网站，现已稳定运行，处于信息系统生命周期的运行和维护阶段。该网站日访问量较大，风险评估工作主要针对这一阶段展开。该 Web 服务器约 3 个月的流量，约有 7 545 228 条访问记录，其中异常记录 350 256 条，按日分布情况见图 2。

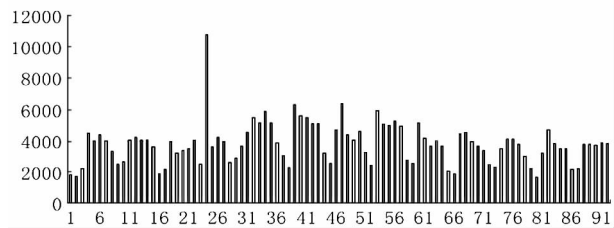

图 2　按日分布情况

根据前一阶段的评估结果，得到不同类型威胁对 WEB 服务器产生的影响值 v_i，如表 1 所示。

表 1　不同类型威胁对 WEB 服务器产生的影响值 v_i

编号 名称	威胁	威胁所利用的脆弱性	影响取值 v_i	风险等级
A_4 WEB 服务器	T_{41}	V_{41}（0.5）	0.3	维护错误
	T_{42}	V_{45}（0.3） V_{46}（0.5）	0.3	系统负载过载
	T_{43}	V_{42}（0.7） V_{43}（0.1） V_{44}（0.5）	0.7	未授权访问系统资源
	T_{44}	V_{45}（0.3） V_{46}（0.5） V_{47}（0.1）	0.5	网络病毒传播
	T_{45}	V_{42}（0.7） V_{43}（0.1） V_{44}（0.5） V_{47}（0.1）	0.7	木马后门攻击 T

法国邮政缩减中期财务目标

日前，鉴于欧洲经济长期萧条、邮件业务量持续下跌等原因，法国邮政决定缩减未来五年内的财务目标，试图借助金融和包裹行业的发展来弥补邮件业务的利润下滑。

在 2013～2018 年“战略计划”中，法国邮政的目标是：到 2018 年，营业利润达到 7.4 亿欧元，营业收入适度增长 1.8％至 240 亿欧元，利润率略有提升。

然而，在之前制定的 2010～2015 年战略基础上，法国邮政想要实现 2015 年 8％的利润率还有很长的路要走。相比之下，法国邮政在 2012 年的营业额出现了 1.5％的略微增长，达到 217 亿欧元，营业利润实现 8.16 亿欧元，利润率达到 3.8％.

即将离任的首席执行官表示，市场环境与 2010 年草拟战略时变化较大。经济危机仍在继续，发展速度依然低迷。此外，邮件量与 2008 年相比下降了约 20％，预计到 2015 年降幅将达到 30％，到 2018 年这一数值将会更高。因此，此时该反思该战略的可行性了。

他强调，近日公布的“共享信心”战略是基于过去几个月对 15.5 万名邮政工人的“大规模咨询”以及面向其他利益相关者召开的多次会议得出的。集团强调要优先考虑员工和客户满意程度。关键的战略支柱在于将法国邮政打造成国内最好的家庭邻里配送服务商、最佳的零售银行以及全球最优秀的包裹快递服务提供商。

他预测，法国邮政的配送服务将会得益于电子商务的发展。这对法国邮政聚焦电子商务和终端投递而言，是一个历史性的机会。集团也在考虑如何使分支网络更好地吸引消费者并提供更多更新的产品和服务。

法国邮政首席财务官强调，这是一个增长性项目，旨在通过略微提高利润率来维持集团的盈利能力。同时，法国邮政仍然计划每年投资 10 亿欧元用于发展业务，包括扩张包裹网络。

考虑到未来五年邮件量可能会出现年均 6％的下降，邮件部门受到的金融影响可能最大。2012 年，该部门的营业利润为 6.84 亿欧元，营业额为 114 亿欧元，占集团总收入的 50％. 到 2018 年，预计该部门营业收入将下跌约 20 亿欧元至 96 亿欧元，比重也缩减到 40％，其营业利润可能出现大幅下跌。

法国邮政正计划大幅调高价格以弥补邮件量下降所造成的收入下降。法国监管机构已经批准在通货膨胀的基础上再上调 1％直至 2015 年；2016～2018 年将上调幅度增加至 3％。据法国媒体透露，这相当于在五年内实现了 24％的整体增长。

然而，首席财务官表示：“与一些欧洲同行相比，法国邮政资费的增长幅度偏低。邮件部门还将继续进行现代化改革，并引进更多的创新服务。”

法国邮政的目标是，到 2018 年，包裹收入提高 25％至 70 亿欧元，年处理量从目前的 10 亿件增长到 13 亿件。届时，包裹收入占集团营业额的比重将从 2012 年的 25％提高到 30％左右，对整个集团的贡献将显著上升。

在 2013～2018 年战略中，法国邮政希望能够通过服务创新和全球网络扩张来提升自己在法国、欧洲和世界各地的竞争力，从而进一步巩固自己作为全球第四大包裹运营商的地位。

法国邮政银行在接受 10 亿欧元的增资后，其业务范围也进一步扩大，为法国消费者提供更多的金融产品和服务。2012 年，该部门营业利润为 6.21 亿欧元，营业收入 52 亿欧元，后者预计将增加到 70 亿欧元左右。预计，公司利润将会随着更多商品的出现而增长。

（朱菁菁　译）

按照公式（3－2），风险值 R_i 计算如下

$$Ri = a_i \times w_i \times \sum_{t_i \in T_a} P(t_i) \times f_i \times \sum_{e_i \in E_a} C(e_i)$$

表 2　不同类型威胁对 WEB 服务器产生的影响值 R_i

威胁类型 T_i	比例 $p(T_i)$	平均日发生次数 $a_i * p(e_i)$	资产权重 w_i	影响取值 $C(e_i)$	损失 R_i
T_{41}	41.01％	1561	0.10	3	468.3
T_{43}	22.91％	872	0.10	70	610.4
T_{44}	18.13％	690	0.30	15	1035
T_{45}	15.31％	583	0.50	35	2040.5
未知	2.63％	100	0.50	25	250

5　结论

建立邮政系统信息化风险控制模型 PS-HRCM 后，通过风险分析与判定以及基于生命周期的风险控制模型的构建，风险管理决策者便能全面掌握组织信息系统当前面临的安全问题。实践证明，PS-HRCM 及其风险量化计算方法，能够有效控制 IT 治理过程中的各种风险，当组织的风险不在安全管理策略设置的安全风险阀值范围内时，可以制定适当的安全方案将信息安全风险控制在可接受范围内。

收稿日期：2013－07－24

作者简介：孟妍（1983～），女，山东济南人，主要从事网络教学研究。