浅谈企业安全度量建设

金融技术部 胡昂

关键词：企业安全技术体系 安全度量 信息安全防护 信息安全决策 态势感知

摘要：基于企业业务对信息化的依赖程度逐步加大，企业安全技术体系建设已经初见成效，信息安全防护手段以消除业务的已 / 未知风险为目标被广泛应用，而众多安全手段的效率、效果乃至成本往往难以被客观的测量和评价，缺失了测量手段和评价制度，将造成企业 IT 技术和管理体系在 PDCA 的持续改进过程中缺乏改进的客观依据。

一、引言

基于企业业务对信息化的依赖程度逐步加大，企业安全技术体系建设已经初见成效，信息安全防护手段以消除业务的已 / 未知风险为目标被广泛应用，而众多安全手段的效率、效果乃至成本往往难以被客观的测量和评价，缺失了测量手段和评价制度，将造成企业 IT 技术和管理体系在 PDCA 的持续改进过程中缺乏改进的客观依据。

管理学中的有句名言：“无法度量的就无法管理”。为了提高企业信息安全工作的有效性和效率，需要针对安全活动和安全防护手段，建立一套可量化、可重复测量的安全指标体系，并通过平台自动化收集和呈现，形成对风险实时和阶段时间内的反馈和针对企业信息系统保障程度的有效度量，最终为信息安全决策和态势感知提供客观的数据支撑。

二、目标

安全度量指标体系

根据行业监管要求、行业规范、外部信息安全状况、企业信息科技管理目标、信息科技管理工作实际情况和行业最佳实践制定企业信息系统安全建设目标、度量指标体系和期望标准。

安全度量系统

依照前期的信息系统安全建设目标、度量指标体系和期望标准，根据信息系统实际情况，建立安全度量系统。度量系统将依照企业的实际需要，实现安全度量信息的收集、计算和展示功能。

三、思路

3.1 安全度量流程

对安全度量的流程，不同的文献和标准中，表述不尽相同，但步骤大体上是相似的。Debra S. Herrmann 认为，安全度量的流

程如下图所示：

NIST SP800-55 Rev1 中，将安全度量的过程分为两个流程：信息安全度量开发流程（如图 1-2 所示）和信息安全度量实施流程（如图 1-3 所示）。

ISO 27004 中，将安全度量分为四个步骤：1）开发测度、2）执行度量项目、3）分析并报告结果、4）对度量项目自身的评估与改进信息安全度量开发流程。

无论怎样表述安全度量的步骤，有两个最关键的步骤是相同的，

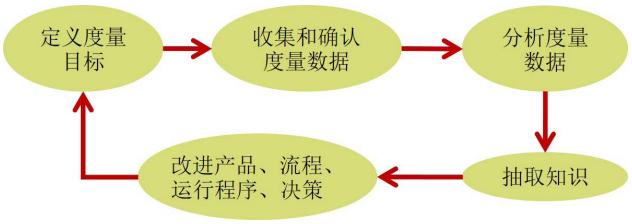

图 1-1 Debra S. Herrmann 的安全度量流程

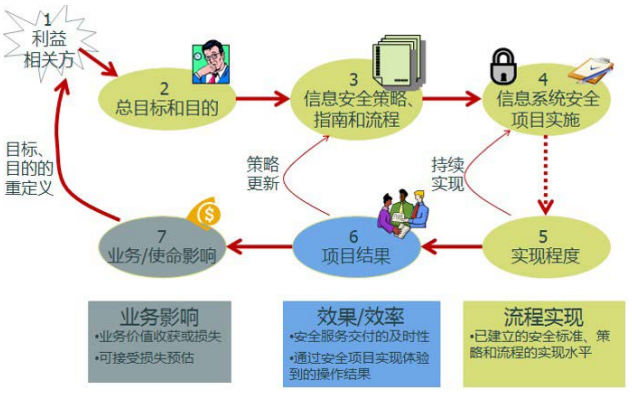

图 1-2 信息安全度量开发流程

图 1-3 信息安全度量实施流程

一个是度量指标的建立，另一个是度量数据的采集。

3.2 安全度量对象

广义上来说，安全度量的对象包含两方面内容：安全控制措施和安全控制目标（资产）。对应安全控制目标的度量，主要度量资产的风险状态。这部分工作有相当部分属于风险识别的范畴。因此一般所说的安全度量，更多的是强调对安全控制措施的度量。但是如果将人员也看作资产的一部分，人员安全也是安全度量的一个重要内容。

本文中，主要侧重在信息资产，人员不作为度量对象的范围。

3.3 安全风险识别

信息安全领域，对风险的计算有着广泛的共识，即风险 = 资产 * 威胁 * 脆弱性，这种表述与风险的分类层次（业务系统 - 场景 - 事件 - 方式）相符合。其中业务系统对应资产，事件对应威胁，方式对应脆弱性。场景是威胁与脆弱性的多重组合。理论上资产根据其重要性，

还应赋予不同的权重系数。本文中，默认所有资产的重要性都是一样的，即权重系数都为 1。同样的，实际的威胁根据其发生的概率和依赖的条件，也应乘以一个系数。这个系数的取值依赖于历史的经验，本文中度量的初始威胁系数都为 1。脆弱性在公开披露时就会被赋予严重等级，根据不同的等级可以赋予其不同的系数。

资产的分类依照实际业务系统的具体情况进行。业界对威胁的分类没有公认的结论，我们根据经验，按照威胁的手法，将威胁分为了六个大类（如图 1-4）：

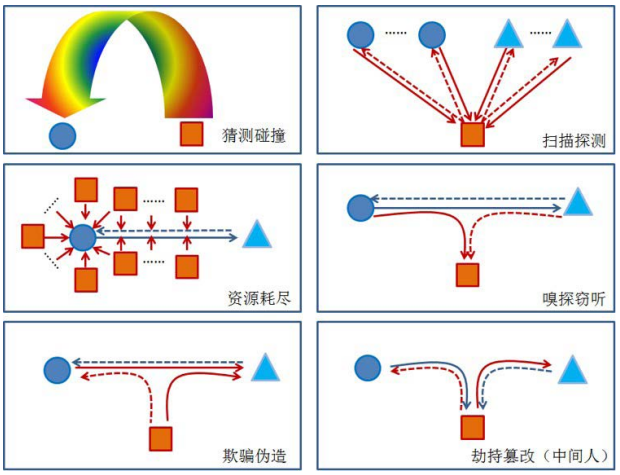

图 1-4 威胁分类模型

3.4 安全控制措施量化

经过多年的信息安全度量实践，不同的组织和学者提出了很多测度指标体系模型，可以用于安全控制措施量化。这些模型大体上可以分为三类，一类是民间的非盈利研究机构提出的模型，一类是基于能力成熟度模型（CMM）的模型，最后一类是一些被广泛应用的标准规范。

企业可参考相关标准规范，并根据自身的实际情况，编制一套适用的安全控制措施量化模型。

3.5 度量结果与呈现

度量的最终结果体现在三个方面：潜在风险、控制能力、残余风险。我们将用从业务系统（资产）的视角才呈现潜在风险（图 1-5 中左侧部分），从不同标准规范的视角呈现控制措施（图 1-5 中右侧和中间部分），用总体态势呈现残余风险（图 1-6）。

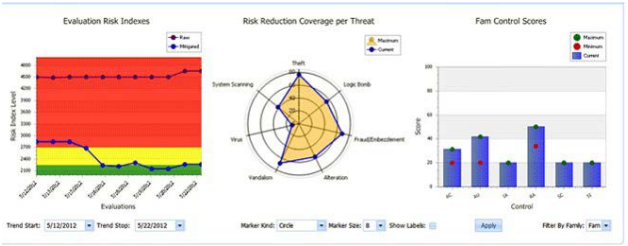

图 1-5

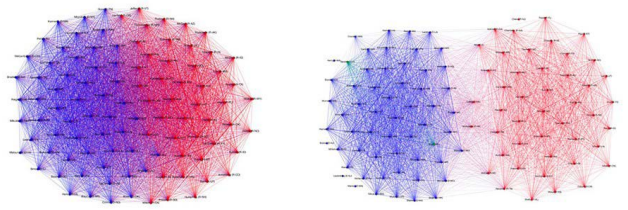

图 1-6 残余风险态势图