第 3 章

网络安全风险

风险(risk)是在 17 世纪 60 年代由意大利语中的 riscare 一词演化而成。它的意大利语本意是在充满危险的礁石之间航行。风险的定义并不统一,部分定义列举如下。

- 风险是某一危险事件发生的频率或者概率与事件后果的组合。在这个定义中,风险与某一特定的危险事件有关。例如某种气体泄漏或者与塔吊坠物有关的风险。但在多种危险事件并存的情况下并不适用。
- 风险是人类活动或者事件造成的后果对现有价值造成伤害的概率。
- 风险是造成资产(包括人员本身)处于危险的情况或者事件,而结果是不确定的。
- 风险是指与资产相关行为的不确定性以及后果(结果)的严重程度。
- 风险是在特定的时间段内,或者由于某种困难情况导致某一负面事件发生的概率。
- 风险是指未来事件和结果的不确定性。它描述了该事件对于完成组织目标产生影响的可能性。
- 风险是给定的威胁源攻击一个特定潜在弱点的可能性,以及此敌对事件对机构产生的影响(NIST SP800-30 给出的定义)。

综上所述,风险定义主要涉及三个方面的问题。

(1) 会发生什么问题? 必须识别出可能会对希望保护的资产造成损害的潜在“威胁事件”。

(2) 发生问题的可能性有多大? 需要逐个考虑问题(1)中的安全事件发生的可能性,进行因果分析,识别出可能导致威胁事件的根本原因(即威胁源)。

(3) 造成的后果是什么? 对于每一个威胁事件,必须识别出潜在的损害及对问题(1)所提出的资产的负面影响。

从以上定义可以看出,网络安全事件发生的可能性是网络安全风险的重要特征。一般认为网络信息系统的安全风险就是一种潜在的、尚未发生但可能发生的安全事件。存在的风险一旦转化为真实的安全事件就会危害网络信息系统的安全性。任何信息系统都会有安全风险,所以,所谓安全的信息系统,实际是指在实施了风险评估并做出风险处置后,仍然存在的残余风险可被接受的信息系统。因此,要追求信息系统的安全,就不能脱离全面、完整的信息系统的安全评估,就必须运用风险评估的思想和规范,对信息系统开展风险评估。所有网络安全建设都应该基于网络安全风险评估。

3.1 网络安全风险构成要素

网络信息系统的安全风险要关注如下基本要素。

- 使命(mission):一个组织机构通过信息化形成的能力所进行的工作任务。

- 依赖度(dependency)：一个组织机构的使命对信息系统和信息的依靠程度。
- 资产(asset)：通过信息化建设积累起来的信息系统、信息以及业务流程改造实现的应用服务的成果、人员能力和赢得的信誉。资产一般可分为逻辑和物理两大类，前者指组织的非物化的智力财富，后者指实物资产。这些资产通常包括系统、硬件、软件、信息、人员等。
- 价值(value)：资产的重要程度。
- 威胁(threat)：指一个威胁源攻击(偶然触发或故意破坏)一个具体弱点的潜在可能性。威胁源指任何可能危害组织资产的环境或事件；威胁是一种可能导致信息安全事件和系统信息资产损失的活动。它利用系统脆弱性来造成后果。威胁的属性包括发起者、动机、目标、可能性和后果等。威胁源是威胁的发起者。按照威胁源性质，威胁一般可分为两类：人为威胁和自然威胁。其中，人为威胁包括人为的故意行为造成的威胁和人为的非故意行为造成的威胁。自然威胁包括系统故障威胁和自然灾害威胁(如雷击、洪水、火灾等)。
- 脆弱性(vulnerability)：指信息系统及其防护措施在安全流程、设计、实现、配置或内部控制中的不足或缺陷，又称为(薄)弱点或漏洞。它是与信息资产有关的弱点、漏洞或安全隐患。脆弱性本身并不对资产构成危害，但是在一定条件得到满足时，脆弱性会被威胁加以利用来对信息资产造成危害。脆弱性包括技术脆弱性、结构脆弱性和组织脆弱性。技术脆弱性主要指由技术方面的因素造成的弱点，如操作系统的漏洞、应用不安全代码编写的应用程序等。它又分为设计弱点、实现弱点和配置弱点。结构脆弱性是指信息系统网络在拓扑结构的设计、布局方面存在的缺陷。组织脆弱性是指系统运行的物理环境、组织制度、业务策略、人事安全、文档管理、安全意识及组织成员培训等组织本身的安全因素存在的缺陷和隐患。
- 可能性(probability)：分威胁利用脆弱性产生安全事件的可能性以及造成影响的可能性，由攻击者的动机、能力、目标资产的价值、脆弱性的诱发条件和已有的安全控制措施等综合因素确定。
- 影响(impact)：对系统的 CIA 等属性和组织的形象、声誉等产生的有形或无形损害；资产价值是影响分析的要素。
- 风险(risk)：本质上就是威胁源利用信息系统脆弱性的可能性与可能产生影响的综合。风险由意外事件发生的概率及发生后可能产生的影响两个指标来衡量。
- 残余风险(residual risk)：采取了安全保障措施，提高了防护能力后，仍然可能存在的风险。
- 安全需求：为保证组织机构的使命正常行使，在信息安全保障措施方面提出的要求。
- 安全保障措施：对付威胁，减少脆弱性，采取预防措施来保护资产和限制意外事件的影响，检测、响应意外事件，促进灾难恢复和打击信息犯罪而实施的各种实践、规程和机制的总称。

这些要素的相互关系如图 3-1 所示。使命由资产支持。资产都有价值，信息化的程

度越高，组织机构的任务越重要，对资产的依赖度越高，资产的价值就越大。资产的价值越大风险越大。风险是威胁发起的，威胁越大风险越大。威胁都要利用脆弱性，脆弱性越大风险越大。脆弱性使资产暴露，威胁利用脆弱性，危害资产，形成风险。人们对风险的意识会引出防护需求，防护需求被防护措施满足。防护措施抗击威胁，降低风险。

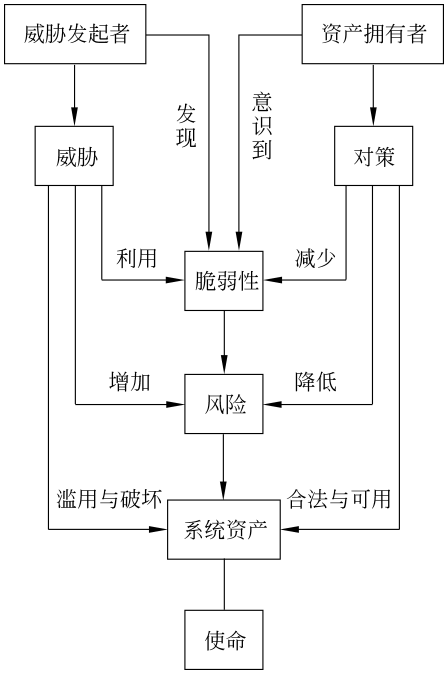

图 3-1　风险各要素之间关系

3.2　网络安全风险管理过程

自从将现代风险理论引入信息安全领域后，国内外许多专家认为，网络安全风险管理是信息安全的基础工作和核心任务之一，是解决网络安全问题的一种最有效措施，是保证网络安全投资回报率优化的科学方法。它是风险评估理论和方法在网络信息系统中的运用，是科学分析理解信息和网络信息系统在机密性、完整性、可用性等方面所面临的风险，并在风险的预防、风险的控制、风险的转移、风险的补偿、风险的分散等之间作出抉择的过程。ISO 31000：2009(风险管理原则与实施指南)标准提供了一个风险管理过程模型，如图 3-2 所示。其中的风险评估可重点参考 NIST SP800-30《风险评估实施指南》，监控与复审可重点参考 NIST SP800-137《信息安全持续监控》和 NIST SP800-55《信息安全性能测量指标》。

风险管理主要包括风险评估和风险处置。风险评估是网络安全的出发点，风险处置是网络安全的落脚点。任何网络信息系统都有安全风险，人们追求的所谓安全的网络信息系统，实际是指网络信息系统在实施风险评估并进行风险处置后，仍然存在的残余风险可被接受的网络信息系统。因此，要追求网络信息系统的安全，就不能脱离全面、完整的

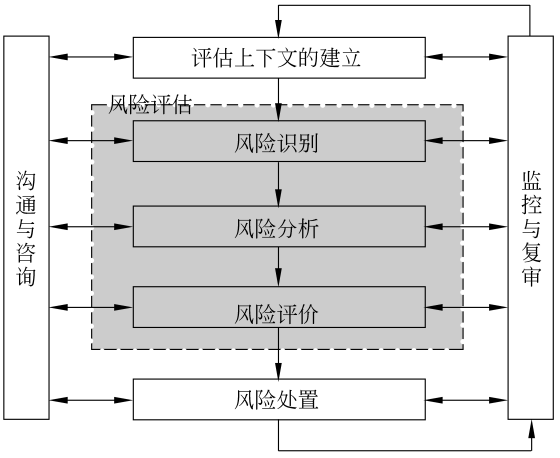

图 3-2 风险管理的过程模型

网络信息系统的安全评估，就必须运用风险评估的思想和规范，对网络信息系统开展风险评估。所有网络安全建设都应该基于安全风险评估。

所谓网络安全风险评估是指依据国家有关技术标准，对网络信息系统的完整性、保密性、可靠性等安全保障性能进行科学、公正的综合评估活动。风险评估可识别系统安全风险并决定风险出现的概率和造成后果的影响，它是风险管理的核心部分。风险评估是对信息及信息处理设施的威胁、影响、脆弱性及三者发生可能性的评估。它是确认安全风险及其大小的过程，即利用适当的风险评估工具，包括定性和定量的方法，确定信息资产的风险等级和风险控制顺序。

一旦威胁源成功地利用信息系统存在的弱点，构成安全事件，就会威胁信息系统的安全。这种威胁将会影响信息资产的机密性、完整性和可用性，并造成资产价值的损失。只有威胁源可能利用脆弱性产生安全事件威胁资产安全时，才能构成风险。因此，网络安全风险可以直观地表示为

$$\text{Risk}=f(\text{Assets},\text{Vulnerabilities},\text{Threats})$$

上式中，Risk 表示风险，Assest 表示资产，Vulnerabilities 表示脆弱性，Threats 表示威胁。

网络安全风险评估就是分析网络信息系统潜在的安全事件及其发生的可能性。考虑风险发生的可能性与风险可能产生的影响，风险还可以表示为事件发生的概率及其后果的函数：

$$\text{Risk}=\text{f}(\text{probability},\text{result})$$

上式中，Risk 表示风险；probability 表示风险发生的可能性，它由存在脆弱性的可能性及威胁被利用的可能性决定；result 表示可能的影响。

函数 f 的计算方法主要有以下两种。

1）矩阵计算法

矩阵内各要素的值根据具体情况采用数学方法确定，然后将两两元素的值放在一个二维矩阵中进行比对，行列交叉处即为所确定的计算结果。后面要介绍的 OWASP、

HEAVENS 等安全风险评估模型就是采用这种计算方法。

2）相乘计算法

当 f 为增量函数时，可以直接相乘，也可以相乘后取模。例如：

$$probability = \sqrt{Threats \times Vulnerabilities}$$

$$result = \sqrt{Assets \times Vulnerabilities}$$

$$Risk = probability \times result$$

需要注意的是，风险评估是预报风险而非预测风险。预测往往带有更强的确定性，而预报不是，存在一定的变数。因此风险评估采用 probability（是否可能发生）而非 possible（是否会发生）来预报风险。风险评估的结果是主观的还是客观的，不在于数据本身是否客观，而在于评估的方法是否科学，以及在相同条件下评估的结果是否可重现？风险评估需要的是准确性（accuracy）而不是精确性（precision），准确性代表一定的范围，精确性代表的是具体的数值。

风险评估又可细分为风险识别、风险分析和风险评价三个环节。

风险识别回答前面提出的第一个问题，目的是找出潜在的可能导致网络信息系统损害的事件。主要包括以下几类识别。

- 资产的识别：攻击点的识别、资产所属信息容器的识别等；
- 威胁的识别：系统遭受攻击的历史、历史安全事件和攻击事件的数据、威胁情报等，包括威胁团体、威胁类型、威胁效果等的识别；
- 脆弱性的识别：以前的风险评估报告、安全检查中发现的问题、系统安全测试的结果等；
- 已有控制措施（及其有效性）的识别：当前及规划中的安全控制措施。

风险分析的目标是结合识别出的资产、威胁、脆弱性和安全控制措施，定性或半定量地综合分析信息网络面临的安全风险，并对风险进行分级。风险分析最常见的定义为：系统地使用既有信息，识别出危险，并预测其对于人员、财产和环境的风险。

从某种意义上说，风险分析是一种主动的方法，目的是避免可能发生的事故。事故调查则与之相反，是一种被动的方法，目的是寻找已经发生的事故原因和情况。

风险分析主要按照如下两个步骤执行，这两个步骤分别对应前面后两个问题的答案。

（1）可能性分析。在这一步中需要进行演绎分析，识别每个威胁事件的成因。同时根据威胁数据和专家判断预测威胁事件的频率。

（2）后果（影响）分析。这个环节需要进行归纳分析，识别所有由威胁事件引起的潜在后果（影响）。归纳分析的目的通常是找出所有可能的最终结果，以及它们发生的概率。

风险分析的方法包括定性分析及定量分析，具体采用哪种方法取决于分析的目标。

- 定性风险分析：以完全定性的方法确定概率和后果。
- 定量风险分析：对概率及后果进行数学估算，有时还需考虑相关的不确定因素。

定量分析适合对那些发生概率较低、影响较大的事件的风险进行量化，也可进行专门的概率评估和大规模分析。

风险评价是在风险分析的基础上，考虑社会、经济、环境等方面的因素，对风险的等

级、组织对风险的容忍度等作出判断的过程。

图 3-3 给出了风险评估的一般流程。

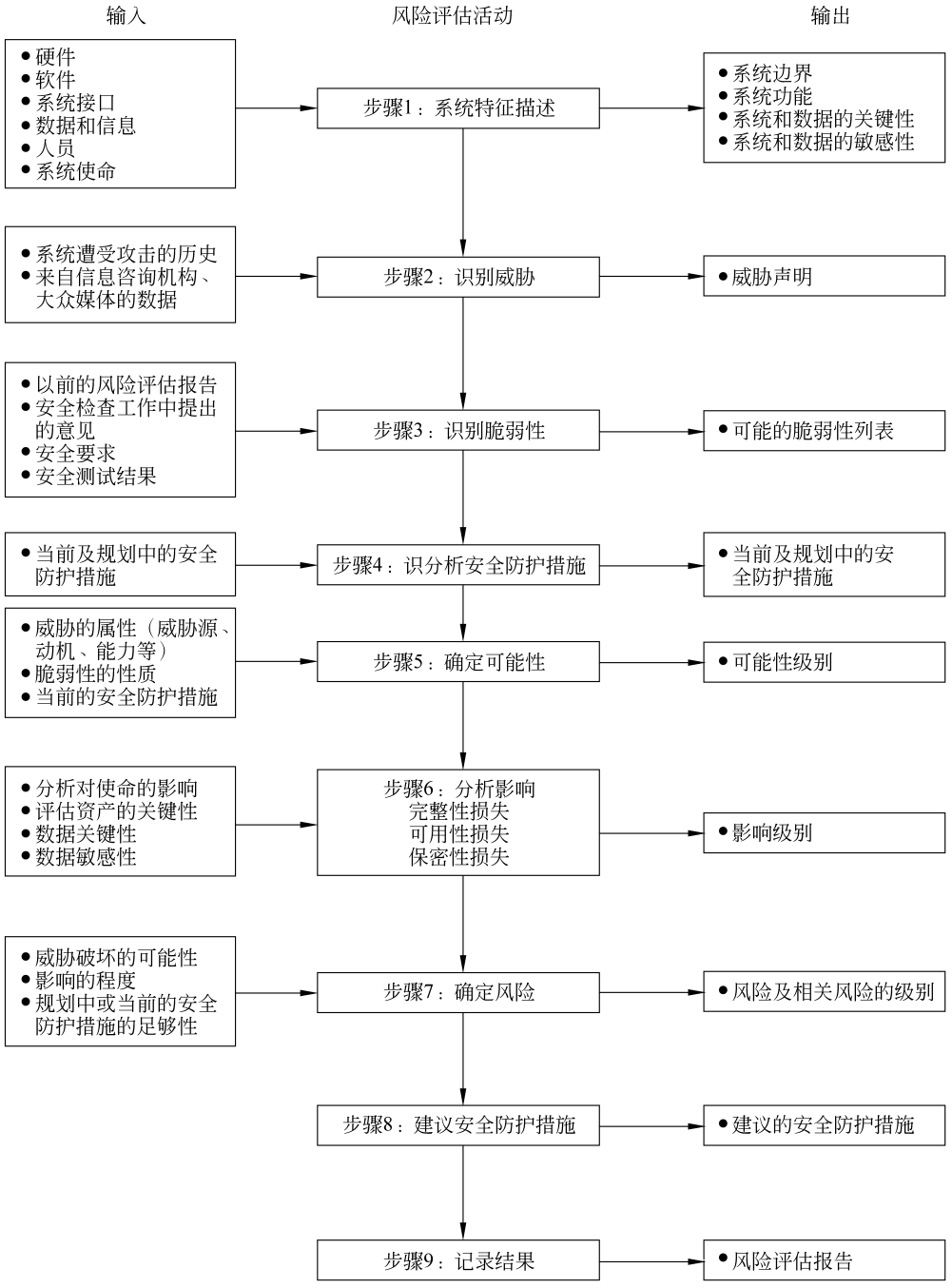

图 3-3　风险评估的一般流程

风险处置就是在风险评估的基础上，采取一系列措施阻止潜在的安全事件发生，如图 3-4 所示。风险处置的目标是针对信息网络面临的风险，按照风险级别的高低提出相

应的风险控制措施和建议，以降低或减缓网络的风险。

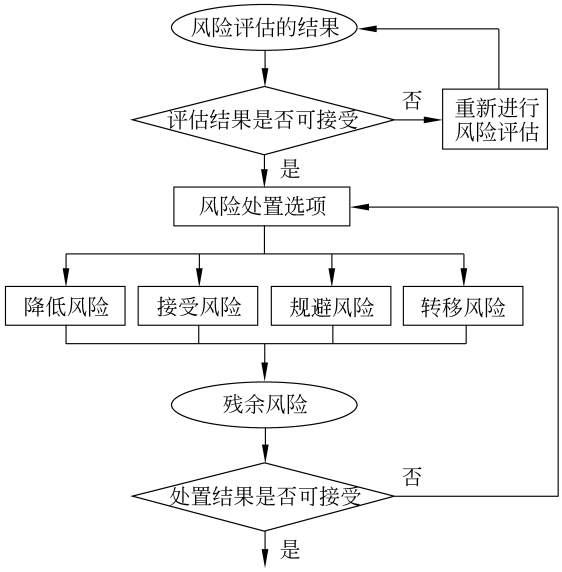

图 3-4　风险处置的流程

风险处置一直采用的方法包括接受风险、转移风险、规避风险和降低风险。因风险存在不确定性，所以无法完全消除。

1）接受风险

接受风险是指如果对于某个风险处置没有很合适的控制措施，或者要采取的控制措施花费太多，得付出难以承担的巨大代价，甚至是得不偿失，那么就可以考虑接受风险的处理方案。由于风险具有不确定性，有风险不意味着就一定发生事故，造成损失。

2）转移风险

转移风险是指将不可接受的风险，全部或部分转给其他方（如保险公司和供应厂商等），由其他方承担全部风险或分担部分风险，是一种把威胁造成的影响连同应对责任一起转移给第三方的风险应对策略。如果选择这个方案，则可采取以下转移风险途径：

- 利用合同；
- 利用保险协议；
- 利用合伙机构或联合其他组织；
- 其他。

3）规避风险

规避风险是指通过计划的变更消除风险或风险发生的条件，保护目标免受风险的影响，是在考虑到某项活动存在风险损失的可能性较大时，采取主动放弃或加以改变的策略，以避免与该项活动相关的风险。

4）降低风险

降低风险是指选择和执行适当的控制措施，将风险减少到可以接受的程度。这是常

用的风险处理方案。

“风险”概念揭示了信息系统安全的本质，它不但指明了信息安全问题的根源，也指出了信息安全解决方案的实质，即把残余风险控制在可接受的水平上。残余风险指采取了安全保障措施，提高了防护能力后，仍然可能存在的风险。

风险是不可完全消除的，对系统采取一定风险处置措施，通过防护措施对资产加以保护，对脆弱性加以弥补，降低风险，那么威胁便会转换为残余风险；而残余风险是可接受的。与此同时，可能有多个防护措施共同起作用，也可能有多个脆弱性被同时利用；有些脆弱性可能客观存在，但是没有对应的威胁，这可能是由于这个威胁不在机构考虑的范围内，或者这个威胁的影响极小被忽略不计。因而，风险是外部威胁和系统脆弱性可能造成损失的潜在危险。风险处置的目标不是消除风险，而是将系统的残余风险控制在组织的风险承受范围之内。

总之，风险评估的结果有利于组织评估与系统信息安全相关的组织治理和管理活动、业务流程、企业架构以及信息安全计划是否合理有效，有利于确定系统安全需求、选择恰当的安全控制措施、监控安全控制措施的执行是否有效。风险处置有利于降低组织的安全风险，将安全风险控制在可接受的范围内。沟通与咨询、监控与复审这两个环节可以将组织层面的风险与系统层面的风险统一起来，使安全风险控制计划融入组织的战略规划中，持续监控安全风险控制的效果，帮助树立对网络信息系统安全的信心。

3.3 网络安全风险评估模型

风险评估是安全需求分析和安全风险管理的核心，为了便于信息安全风险评估工作的展开，国外信息安全专家提出了多种著名的风险评估模型，常见的网络安全风险评估模型包括 PASTA(攻击模拟和威胁分析过程)、OWASP 风险评级模型、HEAVENS(风险分析模型)、OCTAVE(可操作的关键威胁、资产和薄弱点评估模型)、TVRA(威胁、脆弱性与风险评估模型)和 FAIR(信息风险因素分析模型)等。

3.3.1 PASTA

PASTA(Process for Attack Simulation & Threat Analysis)采用以攻击者为中心的视角，从战略到技术层面分析网络信息系统面临的安全威胁和风险，并提出针对性的防范措施。该流程采用了多种分析方法，如攻击树分析、原因结果分析、业务影响分析、CVSS 打分等(详见 3.5 节)。PASTA 的分析流程如图 3-5 所示。

阶段 1：确定目标

- 输入：业务需求文档、功能需求文档、信息安全策略、行业要求的安全标准和指南、数据分类文档；
- 任务：确定业务目标、确定安全需求、确定合规需求、完成初步的业务影响分析；
- 输出：应用功能描述、业务目标列表、应用安全及合规需求说明、业务影响分析报告。

阶段 2：确定技术范围

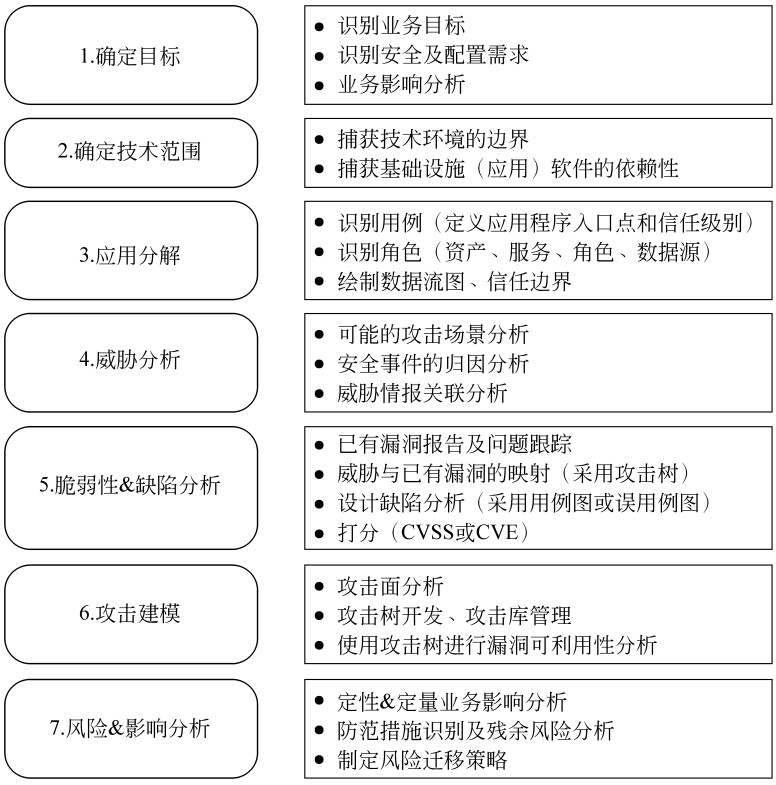

图 3-5　PASTA 流程

- 输入：顶层设计文档、网络拓扑图、逻辑及物理结构图、软件及技术说明书；
- 任务：确定应用边界、识别应用对网络环境的依赖关系、识别应用对服务器和基础设施的依赖关系、识别应用对软件的依赖关系；
- 输出：顶层的、端到端的视图，所有协议及数据的列表，所有应用服务器的列表，所有主机及服务器的列表，软件/技术依赖类型，所有网络设备/配件的列表。

阶段 3：应用分解

- 输入：体系架构图设计文档、时序图、用例，用户、角色及权限，逻辑图，物理网络图；
- 任务：绘制数据流图和信任边界，识别用户/角色及角色的权限，识别资产、数据、服务、硬件及软件，识别数据入口点及信任等级；
- 输出：数据流图，访问控制矩阵，包含数据及数据源的资产列表，接口及信任等级列表，包含角色及资产的用例图。

阶段 4：威胁分析

- 输入：威胁源及其动机，安全事件报告，安全事件监控报告（SIEM），应用及服务器日志，威胁情报报告；
- 任务：分析攻击场景的可能性，分析事件管理报告，分析应用日志及安全事件，将威胁情报与事件关联起来；

- 输出：攻击场景报告，威胁源及攻击列表，安全事件与威胁场景的可能性分析，攻击场景与威胁情报的关联分析。

阶段 5：脆弱性及缺陷分析

- 输入：攻击树，攻击场景，漏洞评估报告，漏洞分级标准，漏洞打分标准；
- 任务：将漏洞与应用资产关联起来，使用攻击树将威胁与漏洞关联起来，使用用例图或误用例图将威胁与安全缺陷关联起来，对脆弱性打分；
- 输出：漏洞与攻击树中节点的映射图，漏洞的打分结果，威胁、攻击、漏洞、资产映射表。

阶段 6：攻击建模

- 输入：应用技术范围，应用分解，攻击库模式，针对应用资产的威胁、攻击和脆弱性列表；
- 任务：识别应用攻击面，根据威胁和资产派生出攻击树，将攻击途径映射到攻击树中的节点，使用攻击树识别出攻击的途径；
- 输出：应用攻击面，针对目标资产的攻击树，包含受影响资产和脆弱性映射关系的攻击树，可能的攻击途径（路径）。

阶段 7：风险及影响分析

- 输入：初步的业务影响分析，技术范围，应用分解，威胁分析，漏洞分析，攻击分析，攻击与控制的映射，控制的技术标准；
- 任务：定性及定量的业务影响分析，识别安全控制的差距，计算残余风险，识别风险迁移策略；
- 输出：应用风险概要文件，定量及定性的风险报告，包含威胁、攻击、脆弱性、业务影响、业务残余风险的威胁矩阵，风险迁移策略选项。

PASTA 计算风险的方法是：

$$\boldsymbol{R}=\left(\frac{\boldsymbol{T}_P \times \boldsymbol{V}_P}{\boldsymbol{C}}\right)\times \boldsymbol{I}$$

其中，T_P：威胁发生的概率；V_P：漏洞利用的概率；C：安全控制措施；I：影响大小。

3.3.2 OWASP

OWASP（Open Web Application Security Project）风险评级模型[①]认为“风险（Risk）＝可能性（Likelihood）×影响（Impact）”。风险评级的流程如下。

步骤一：确定风险。收集涉及的攻击者、攻击方法、利用漏洞和业务影响方面的信息。

步骤二：评估可能性。确定潜在风险后，需要评估风险有多严重，第一步是评估它发生 的可能性。“发生的可能性”可按“低、中、高”分等级粗略估量。有很多因素可以帮助分析“发生的可能性”。第一类相关因素就是攻击者。这一步的目标是估计一个可能发起

① OWASP Threat Dragon 是一种建模工具，用于在安全开发生命周期中创建威胁模型图，https://owasp.org/www-project-threat-dragon/。

攻击的团体成功攻击的可能性。举例来说，内部人员可能比外部人员更可能成为攻击者——这取决于多种因素。每个因素都有一系列选项，每个选项都有“发生的可能性”。可以使用0～9的数字评估最后的可能性。评估“发生的可能性”涉及的主要因素列举如下。

1）攻击者因素：评估攻击者成功攻击的可能性。

- 攻击者的技术水平（技术水平）：（1）不具备能力（1分）；（2）具备初级能力（3分）；（3）高级计算机使用者（4分）；（4）具备网络和编程能力（6分）；（5）具备渗透能力（9分）。
- 攻击者发现和利用漏洞的动机（动机）：（1）低或者零回报（1分）；（2）可能带来回报（4分）；（3）很高的回报（9分）。
- 攻击者寻找和利用某个漏洞的成本有哪些（机会）：（1）完全访问权限或高昂的成本（0分）；（2）特定访问权限或较高的成本（4分）；（3）部分访问权限或一般的成本（7分）；（4）无须访问权限或者没有成本（9分）。
- 攻击者的人员构成有哪些（规模）：（1）开发者（2分）；（2）系统管理员（2分）；（3）内部用户（4分）；（4）合伙人（5分）；（5）认证用户（6分）；（6）匿名互联网用户（9分）。

2）漏洞因素：评估特定的漏洞被发现和利用的可能性。

- 攻击者发现这个漏洞难易程度如何（发现难易程度）：（1）几乎不可能（1分）；（2）困难（3分）；（3）容易（7分）；（4）可以使用自动化工具（9分）。
- 攻击者实际利用这个漏洞的难易程度如何（利用难易程度）：（1）几乎不可能（1分）；（2）困难（3分）；（3）容易（5分）；（4）可以使用自动化工具（9分）。
- 漏洞在攻击者中存在的知晓率（知晓度）：（1）未知的（1分）；（2）有隐蔽性的（4分）；（3）比较显著的（6分）；（4）众所周知的（9分）。
- 漏洞被利用后如何检测（入侵检测）：（1）应用程序主动发现（1分）；（2）日志记录和审核（3分）；（3）日志记录（8分）；（4）没有日志（9分）。

步骤三：评估影响。当考虑成功攻击的影响时，关键要意识到有两类影响。第一类对应用程序所使用的数据以及它所提供的功能的“技术影响”。第二类是对该组织开展相关业务应用的“业务影响”。评估影响涉及的主要因素列举如下。

1）技术影响因素。技术影响由多个因素组成并和传统的安全考虑相一致，即保密性，完整性，可用性以及可追溯性。目标是评估漏洞被利用后对系统影响的大小。

- 有多少信息被泄露，敏感程度如何（损失保密性）：（1）少量不敏感信息被泄露（2分）；（2）少量关键数据被泄露（6分）；（3）大量不敏感信息被泄露（6分）；（4）大量敏感信息被泄露（7分）；（5）所有数据丢失（9分）。
- 有多少数据被破坏，破坏的程度如何（损失完整性）：（1）少量轻微的数据被破坏（1分）；（2）少量严重的数据被破坏（3分）；（3）大量轻微的数据被破坏（5分）；（4）大量严重的数据被破坏（7分）；（5）所有数据完全彻底被破坏（9分）。
- 有多少服务会被中断，重要程度如何（损失可用性）：（1）少量二线服务被中断（1分）；（2）少量主要服务被中断（5分）；（3）大量二线服务被中断（5分）；（4）大

量主要服务被中断(7 分);(5)全部服务被中断(9 分)。

- 攻击者的行动是否能追溯到个人(损失问责性):(1)完全可追溯(1 分);(2)可能可追溯(7 分);(3)完全匿名(9 分)。

2) 业务影响因素。业务影响源于技术影响,但是需要进一步理解对于组织应用来说什么重要。

- 在一次漏洞被利用的事件里,财务损失情况如何(财务损失):(1)损失少于修复漏洞的成本(1 分);(2)对于年收益影响很小(3 分);(3)对年收益影响显著(7 分);(4)破产(9 分)。
- 漏洞被利用是否会对业务造成声誉损失(声誉损失):(1)很小的损失(1 分);(2)损失主要客户(4 分);(3)损失发展前景(5 分);(4)失去品牌(9 分)。
- 不合规的程度(不合规):(1)很小的违反(2 分);(2)明显的违反(5 分);(3)严重的违反(7 分)。
- 多少个人身份信息被泄露(侵犯隐私权):(1)一个人(3 分);(2)百余人(5 分);(3)千余人(7 分);(4)百万人(9 分)。

步骤四:确定风险的严重程度。把可能性评估和影响评估放在一起,计算风险的总体严重程度。明确可能性和影响的低、中或者高影响度。

首先是选择与每个因素相关的选项,并在表中输入关联的编号。然后,计算各因素得分的平均数作为总体的可能性。示例如表 3-1 所示。

表 3-1 确定风险发生的可能性举例

攻击者因素				漏洞因素			
技术水平	动机	机会	规模	发现难易程度	利用难易程度	知晓度	入侵检测
5	2	7	1	3	6	9	2
总体的可能性=4.375(中)							

接下来,需要搞清风险的整体影响,这与上述流程相似。在许多情况下,答案是显而易见的,但也可以根据具体的因素估计,计算每个因素的平均得分,小于 3 为低影响,3 至 6(不含 6)为中等影响,6 至 9 为高影响。示例如表 3-2 所示。

表 3-2 确定风险造成的影响举例

技术影响				业务影响			
损失保密性	损失完整性	损失可用性	损失问责性	财务损失	声誉损失	不合规	侵犯隐私
9	7	5	8	1	2	1	5
整体技术影响=7.25(高)				整体业务影响=2.25(低)			

然后采用风险严重程度评估矩阵,确定风险的严重等级,如表 3-3 所示。

表 3-3　风险严重程度评估矩阵

整体风险的严重程度				
影响	高	中	高	关键
	中	低	中	高
	低	注意	低	中
		低	中	高
	可能性			

上述示例的风险发生的可能性为中等，其风险造成的技术影响为高等，因此从纯技术的角度来看，似乎整体风险严重程度为高。但是，因为该漏洞对实际业务的影响是低的，所以整体的风险严重程度应该为低。这说明在评估漏洞时，了解其对实际业务环境的真实影响非常重要。

步骤五：决定修复内容。在完成风险分类后，应该首先修复最严重的风险。

步骤六：定制风险评级模型。拥有一个定制的风险评级框架对于业务至关重要。量身打造的模型可能更加符合组织对严重风险的看法。可以根据需要增加新的评价因素，或者调整现有评价选项的得分。此外，上述模型并没有考虑各选项的计算权重，而是直接采用算术平均的方法。还可以根据需要采取加权平均的计算方法计算风险发生的可能性和影响的大小。

3.3.3　HEAVENS

HEAVENS风险分析模型是瑞典专家针对汽车电子电气系统威胁分析和风险分析提出的模型，它提供了一套完整的风险评估流程，以威胁为中心，同时采用了微软的STRIDE方法对系统进行威胁评估。评估流程主要分为三个阶段：威胁分析、风险评估和安全需求确定。威胁分析主要通过评估对象或功能的典型应用场景，将威胁与评估对象、安全属性进行映射，形成对应关系；风险评估主要对威胁与评估对象进行等级划分，具体是通过综合考虑威胁等级和影响等级两个维度实现安全等级的划分；最后再将威胁、评估对象、安全属性和安全等级这四个维度进行整合形成安全需求。开发人员根据安全需求与安全等级最终确定开发的优先级，如图 3-6 所示。

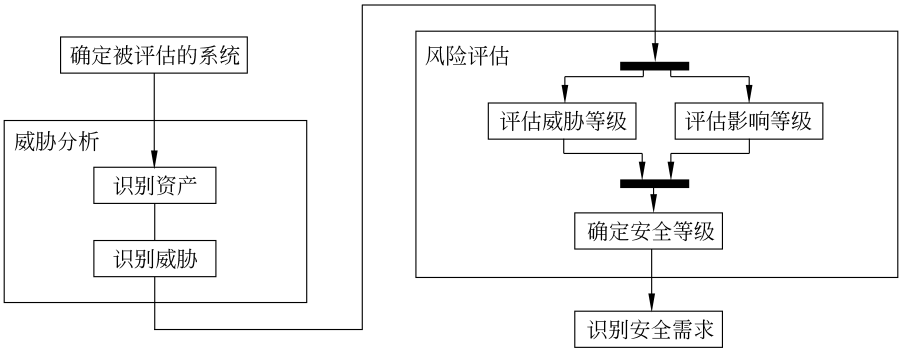

图 3-6　HEAVENS 评估流程

威胁分析是指识别与评估与资产相关的威胁以及威胁与安全属性的映射。威胁分析的输入为评估对象描述与功能应用场景，产生两个输出：①威胁和资产之间的映射关系；②威胁和安全属性之间的映射关系，以确定资产上下文中的特定威胁会影响哪些安全属性。

HEAVENS采用微软的STRIDE方法对威胁进行分析。STRIDE通过将威胁与安全属性关联起来，提供扩展CIA（保密性，完整性，可用性）原始模型的机会（真实性、完整性、不可抵赖性、机密性、可用性、新鲜度和授权）。

每一类的STRIDE威胁被静态地映射到一组安全属性，用于表示在风险评估期间，一旦确定了特定（威胁-资产）对的安全等级，就可用于确定网络安全需求。

确定评估对象的安全威胁后，就进入到了风险评估环节，进而需要确定威胁的等级和威胁对评估对象造成的影响等级。不论是威胁等级的评定还是影响等级的评定，都是针对具体的安全防护目标（资产）而言的。表3-4给出了评定威胁等级需要考虑的参数，其中威胁的机会窗口反映的是系统（网络）脆弱性和相应已经采取的安全控制措施的综合分析得到的结果。

表3-4 评定威胁等级的参数

参数	值	参数	值	参数	值	参数	值
专业技能（x）		对系统的了解（k）		机会窗口（w）		装备（e）	
门外汉	0	公开的	0	很大	0	标准的	0
熟练工	1	受限的	1	大	1	特殊的	1
专家	2	敏感的	2	中	2	需定制开发	2
多面手专家	3	关键的	3	小	3	需多领域定制开发	3

各参数的具体含义如下。

（1）专业技能。

- 门外汉：不需要特别的专业知识；
- 熟练工：需要通用的安全和领域知识，是具有简单知识的专业人员，掌握流行的攻击，能够使用可用的工具，并且在必要时即兴发挥；
- 专家：需要专家级的安全和领域知识，熟悉底层算法、协议、硬件、软件和概念，掌握攻击技术和现有的工具，并能够创建新的攻击；
- 多面手专家：掌握安全和多领域的知识，在某种情况下能够运用不同的专业领域知识实施攻击并取得成功。

（2）对系统的了解。

- 公开的：必要的信息都是公开的；
- 受限的：与合作伙伴共享的信息受保密协议限制；
- 敏感的：信息在特定团队之间共享，但访问仅限于其成员；
- 关键的：信息仅限于很少的人共享，访问按照需要原则受到严格的控制。

(3) 机会窗口。

- 很大：无限制的物理访问，或无限的网络访问时间；
- 大：具有很高的物理和/或远程访问可用性，但有一些时间限制；
- 中：可用性低，存在严重的时间限制。对目标的物理和/或远程访问有限。无须使用任何特殊设备/工具即可接触物理网络/系统；
- 小：可用性非常低。需要物理访问内部网络/系统，并对资产发起攻击。

(4) 装备。

- 标准的：攻击者可以随时获得这些装备，装备可以是目标本身的一部分(例如操作系统中的调试器)，或者很容易获得；
- 特殊的：攻击者不容易获得该装备，但可以在不过度努力的情况下获得，可能包括购买适量的装备，或开发更适用的攻击脚本；
- 需定制开发：该装备不易向公众提供，因为它可能需要专门生产，或者因为装备非常专业化，其分布受到控制或限制，或者装备可能非常昂贵，需要多种类型的专用设备；
- 需多领域定制开发：需要多种类型的定制装备才能成功攻击。

威胁等级的划分参考表3-5确定。

表3-5　威胁等级的划分

威胁等级各参数的值	威胁等级(TL)	TL值
＞9	无	0
7～9	低	1
4～6	中	2
2～3	高	3
0～1	非常高	4

最终的威胁值的计算采用如下公式。

$$T_{sum}=w_x t_x+w_k t_k+w_w t_w+w_e t_e$$

式中，w 为指标权重，各指标权重的确定可以采用熵权法或AHP(Analytic Hierarchy Process)法。

1. 熵权法

熵最先由香农引入信息论，并在工程技术、社会经济等领域得到非常广泛的应用。熵权法的基本思路是根据指标变异性的大小来确定客观权重。一般来说，若某个指标的信息熵越小，表明指标值的变异程度越大，提供的信息量越多，在综合评价中所能起到的作用也越大，其权重也就越大。相反，某个指标的信息熵越大，表明指标值的变异程度越小，提供的信息量也越少，在综合评价中所起到的作用也越小，其权重也就越小。熵权法的计算步骤如下。

步骤一：确定指标。如下所示的矩阵 $X_{n\times m}$，矩阵中的列表示各项评估指标(共有 m 项指标)，行表示某位专家(共有 n 位专家参与打分)，矩阵中的元素 X_{ij}($i=1,2,\cdots,n$，j

$=1,2,\cdots m$)代表专家 i 对指标 j 的打分值。

$$X_{n\times m}=\begin{bmatrix} X_{11} & X_{12} & \cdots & X_{1m} \\ X_{21} & X_{22} & & \cdots X_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ X_{n1} & X_{n2} & \cdots & X_{nm} \end{bmatrix}$$

步骤二：指标归一化处理。

正向指标(越大越好)：

$$X_{ij}=\frac{X_{ij}-\min\{X_{1j},\cdots,X_{nj}\}}{\max\{X_{1j},\cdots,X_{nj}\}-\min\{X_{1j},\cdots,X_{nj}\}}$$

负向指标(越小越好)：

$$X_{ij}=\frac{\max\{X_{1j},\cdots,X_{nj}\}-X_{ij}}{\max\{X_{1j},\cdots,X_{nj}\}-\min\{X_{1j},\cdots,X_{nj}\}}$$

步骤三：计算第 j 项指标下第 i 个样本值占该指标的比重。

$$P_{ij}=\frac{X_{ij}}{\sum_{i=1}^{n}X_{ij}},\quad i=1,2,\cdots,n;j=1,2,\cdots,m$$

步骤四：计算第 j 项指标的熵值。熵是 1948 年香农提出的信息论中的一个概念，它被用来度量事物的不确定性。即信息量越大，越具有确定性，熵的值就越小；反之，信息量越小，越具有不确定性，熵的值就越大。

$$e_j=-k\sum_{i=1}^{n}P_{ij}\ln(P_{ij}),j=1,2,\cdots,m$$

其中，$k=\frac{1}{\ln(n)}>0$，所以满足 $e_j\geqslant 0$。若 $P_{ij}=0$，定义 $e_j=0$。

步骤五：计算信息熵冗余度。

$$d_j=1-e_j,\quad j=1,2,\cdots,m$$

步骤六：计算各项指标的权重。

$$w_j=\frac{d_j}{\sum_{j=1}^{m}d_j},\quad j=1,2,\cdots,m$$

利用熵权法客观测出各项指标所占的权重 w_j，其中，e_j 值越接近 1，说明熵权法的使用越科学。

2. AHP 法

AHP(Analytic Hierarchy Process)法和 Delphi 法相结合也可以用于确定各项指标的权重。AHP 是 20 世纪 70 年代美国国防部研究“根据各个工业部门对国家福利的贡献大小而进行电力分配”课题时提出的一种层次权重决策分析方法。AHP 将与决策总是有关的元素分解成目标、准则、方案等层次，并在此基础之上进行定性和定量分析。

AHP 法确定权重的方式如下。

步骤一：构建指标的判断矩阵。

构建判断矩阵时，不要把所有指标放在一起比较，而是两两比较；比较时采用相对尺

度，以尽可能减少性质不同的诸指标相互比较的困难，提高准确性。常用的判断取值法如表 3-6 所示。

表 3-6　指标比较重要度相对取值法

标　　度	含　　义
1	表示两个因素相比，具有同样重要性
3	表示两个因素相比，一个因素比另一个因素稍微重要
5	表示两个因素相比，一个因素比另一个因素明显重要
7	表示两个因素相比，一个因素比另一个因素强烈重要
9	表示两个因素相比，一个因素比另一个因素极端重要
2，4，6，8	上述两相邻判断的中值
倒数	因素 i 与 j 比较的判断 a_{ij}，则因素 j 与 i 比较的判断 $a_{ji}=\dfrac{1}{a_{ij}}$

矩阵的判断值可以通过专家讨论得出。为方便讨论，这里选择模拟一个相对重要度判断的情况，以获得各部分的判断矩阵，如表 3-7 所示。表中 N_i 表示指标 i，m 项指标就构成一个 $m\times m$ 的判断矩阵，矩阵的元素 x_{ij} 表示指标 N_i 对指标 N_j 的相对重要度。

表 3-7　各指标的判断矩阵示例

x_{ij}	N_1	N_2	N_3
$N1$	1	2	3
$N2$	1/2	1	2
$N3$	1/3	1/2	1

步骤二：计算各层的相对权重。以表 3-7 所示的矩阵为例，分别进行如下计算。

(1) 归一化各判断值。

$$h_{ij}=\frac{x_{ij}}{\sum_{i=1}^{m}x_{ij}}$$

因此得到：

$$h_{11}=\frac{1}{\left(1+\frac{1}{2}+\frac{1}{3}\right)}=0.535,\ h_{21}=\frac{\frac{1}{2}}{\left(1+\frac{1}{2}+\frac{1}{3}\right)}=0.263,$$

$$h_{31}=\frac{\frac{1}{3}}{\left(1+\frac{1}{2}+\frac{1}{3}\right)}=0.182$$

$$判断矩阵\ H=\begin{bmatrix}0.535 & 0.571 & 0.5\\ 0.263 & 0.286 & 0.333\\ 0.182 & 0.153 & 0.167\end{bmatrix}$$

(2) 将判断矩阵 H 按行相加。

$$h_i=\sum_{j=1}^{m}h_{ij},i=1,2,\cdots,m$$

计算可得：

$$h_1=0.535+0.571+0.5=1.606$$
$$h_2=0.263+0.286+0.333=0.882$$
$$h_3=0.182+0.153+0.167=0.502$$

(3) 计算权重向量。

$$h_i^o=\frac{h_i}{\sum_{i=1}^{m}h_i}$$

可得判断矩阵的特征向量：

$$h_1^o=\frac{1.606}{1.606+0.882+0.502}=0.539$$
$$h_2^o=\frac{0.882}{1.606+0.882+0.502}=0.297$$
$$h_3^o=\frac{0.502}{1.606+0.882+0.502}=0.164$$

最终获得：

$$H=[0.539\quad 0.297\quad 0.164]$$

如果有 n 个专家对相同的指标进行判断，可以利用 Delphi 法进行综合，得到最终的指标权重：

$$w_j=\frac{\sum_{i=1}^{n}H_{ij}}{n}$$

其中，w_j：指标 j 的权重；H_{ij}：专家 i 对指标 j 的权重判断值；n：专家总数。

完成威胁等级评定后，HEAVENS 模型中影响等级的评定需要考虑的参数如表 3-8 所示。

表 3-8 评定影响等级的参数

参数	值	参数	值	参数	值	参数	值
安全性 (safety)		经济性 (financial)		业务影响 (operational)		合规性 (privacy & legislation)	
无伤害	0	低成本	0	低	0	不违反	0
较小的伤害	10	一般成本	10	中	10	低	1
严重伤害	100	高成本	100	高	100	中	10
非常严重伤害	1000	很高成本	1000			高	100

影响等级的划分参考表3-9确定。

表3-9 影响等级的划分

影响等级各参数的值	影响等级(IL)	IL值
0	无	0
1～19	低	1
20～99	中	2
100～999	高	3
＞＝1000	非常高	4

最终影响值的计算采用如下公式：

$$I_{sum} = w_s i_s + w_f i_f + w_o i_o + w_p i_p$$

式中的 i_s、i_f、i_o、i_p 分别表示对系统安全性、经济性、业务和合规性等造成的影响，而 w_s、w_f、w_o、w_p 分别是各项指标所占的权重，且权重和为1。

分析影响等级时可能会存在以下不确定性。

- 不确定：系统会不会被攻击？攻击会不会成功？攻击成功会不会造成实际损失？
- 太复杂：最典型的影响(如数据泄露)被媒体报道时，声誉损失要怎么算？
- 数据少：重大事件原本就少，被攻击的组织又通常不会公开数据。

在确定威胁等级和影响等级后，就可以采用如表3-10所示的映射矩阵，确定评估对象的安全等级。需要注意的是，表中的安全等级越低，说明其面临的安全风险越低，反之则越高。

表3-10 安全等级的评定矩阵

安全等级(SL)	影响等级(IL)					
威胁等级(TL)		0	1	2	3	4
	0	很低	很低	很低	很低	低
	1	很低	低	低	低	中
	2	很低	低	中	中	高
	3	很低	低	中	高	高
	4	低	中	高	高	很高

3.3.4 OCTAVE

可操作的关键威胁、资产和薄弱点评估(Operationally Critical Threat, Asset, and Vulnerability Evaluation, OCTAVE)是由美国卡耐基-梅隆大学软件工程研究所下属的CERT协调中心开发的用以定义一种系统的、组织范围内的评估信息安全风险的模型。其主要流程如图3-7所示。

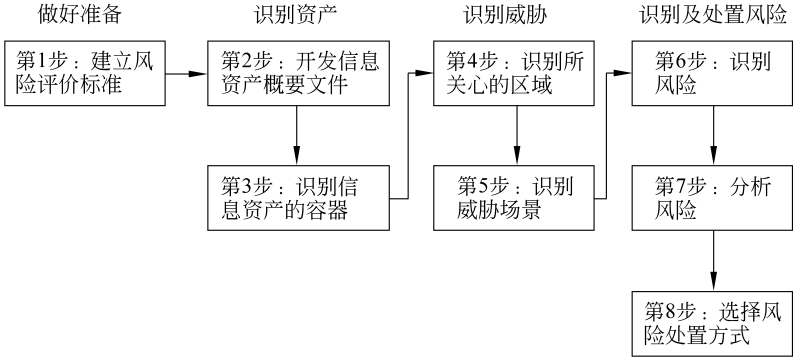

图 3-7　OCTAVE 风险评估流程

1）阶段一：建立基于资产的威胁概要文件

- 目标：建立组织对信息安全问题的概括认识。
- 任务：首先需要收集组织内工作人员对信息安全风险问题的个人看法和观点，然后对这些不同的个人看法观点进行综合梳理，为评估过程中的所有后续分析活动打下基础。

通过对组织专业领域知识的调查研究，工作人员能够搞清楚信息资产、资产面临的威胁，资产的安全需求，组织当前实行的保护信息资产的措施，以及组织资产和措施的缺点等有关问题。

- 过程：

过程 1　标识高层管理部门的知识。明确高级管理层对组织重要资产的认识，了解资产是如何受到威胁的，了解资产的安全需求，以及当前资产已经采取的保护措施和保护该资产相关的问题。

过程 2　标识业务区域管理部门的知识。明确执行经理层对组织重要资产的认识，了解资产是如何受到威胁的，了解资产的安全需求，以及当前资产已经采取的保护措施和保护该资产相关的问题。

过程 3　标识员工的知识。明确员工层对组织重要资产的认识，了解资产是如何受到威胁的，了解资产的安全需求，以及当前资产已经采取的保护措施和保护该资产相关的问题。

过程 4　建立基于资产的威胁概要文件。根据过程 1～3 明确组织的关键资产，描述关键资产的安全需求，标识关键资产面临的威胁。

2）阶段二：识别基础设施的薄弱点

- 目标：完成当前信息基础设施的评价。
- 任务：通过检查其中的关键运行组件，发现导致非授权行为的相关漏洞（技术脆弱性）。
- 过程：

过程 5　标识重要资产的关键组件。识别重要资产的关键组件，然后用适当的方法和有效的工具对其进行脆弱性的评估。

过程 6　评估选定的组件。识别技术上的脆弱性，并对结果进行总结和摘要。