首席安全官（CISO）应用安全指南

Version 1.0 (November 2013)

项目负责人及主要作者

Marco Morana

合著者，提供者和审阅

Tobias Gondrom, Eoin Keary, Andy Lewis, Stephanie Tan and Colin Watson

翻译者

樊山、贺新朋、胡晓斌、郝轶、陈东、陈亮

首席安全官们（CISO）负责从治理、合规性和风险的角度对待应用的安全性。首席安全官应用安全指南旨在帮助CISO根据自己的角色、职责、观点和需要管理应用安全计划。应用安全最佳实践和OWASP的资源在整个指南中被引用。

前言

本指南已经得到了OWASP的项目重启计划的支持，并且符合OWASP的核心价值，指南的开发体现内容的开放性、创新性的想法和概念，将完整内容发布给遍及全球的应用安全领域内严格中立和无特定商业利益偏向的供应商。该指南还开发有关OWASP核心价值如能“促进实施和促进遵守的标准、程序和应用安全控制”，并提供免费和开放的内容，在不以盈利为目的的OWASP原则下提高基于风险的应用安全方法。CISO OWASP应用安全指南项目的领导者是Marco Morana。Colin Watson, Eoin Keary, Tobias Gondrom和Stephanie Tan为本指南的原始内容的开发做出贡献。。这个项目是OWASP与CISO调查项目负责人Tobias Gondrom同时开发。

同步运行这两个项目的目标是使用2013 CISO调查结果，并通过强调其中的OWASP项目/资源解决这些需求，进而通过具体的CISO的需求定制指南。OWASP首席安全官应用安全指南2013年11月版在2013年美国APPSEC大会提出，该会议在2013年11月18日至23日纽约举行。

手册序言

简介

应用安全的利益相关者中，CISO（CISO）负责从治理、合规性和风险的角度考虑应用安全性。本指南旨在帮助CISO根据CISO的角色、职责、观点和需要来管理应用安全计划。本指南中引用应用安全最佳实践和OWASP的资源。OWASP是一个非赢利组织，其宗旨是“使应用程序的安全可见，并赋予应用安全与利益相关者正确的信息，并用于管理应用程序的安全风险”

本指南可帮助CISO从信息安全和风险管理的角度管理应用安全计划。从信息安全的角度来看，对组织的资产进行保护是很有必要的，这些资产包括公民、客户端和客户敏感数据，存储这些数据的数据库,数据库服务器所在的基础设施，以及最后也是最重要的用于访问和处理这些数据的应用和软件。除了业务和用户数据，应用程序和软件也是CISO要保护的资产。其中一些应用程序和软件为组织产生了收益并为客户提供关键业务功能。例如，为客户提供商务服务以及应用和软件，为客户销售产品的应用和软件。在软件应用被认为是业务关键信息资产的情况下，这些应该在人力资源、培训、流程、标准和工具中得到特别的关注。本指南的范围是Web应用安全和结构与组件的安全，如Web服务器，应用服务器和数据库的安全；这不包括其他不相关的具体应用的安全。例如，支撑应用和构成一个有价值的资产的网络基础设施的安全属性，如保密性，完整性和可用性同样需要得到保护。

（樊山）

目标

本指南能够帮助CISO从曝光的新威胁和合规性要求方面考虑管理应用安全风险。该指南可以帮助CISO们：

- 使应用安全对CISO可见
- 确保应用符合隐私安全、数据保护和信息安全相关法规

- 优先修复有风险的业务漏洞
- 为构建应用安全提供指导意见
- 分析针对应用的网络威胁并找出对策
- 衡量和管理应用安全风险和流程

受众群体

- CISO
- 高级安全经理
- 高级技术经理

（胡晓斌）

内容摘要

事实上，应用应该被视为组织的资产，这“本身”就是一个把应用界定在符合信息安全策略和标准之内的很好的理由。应用是否符合信息安全策略和标准通常取决于存储在应用中的资产数据的分类，暴露给用户的应用类型（例如互联网、内联网、外联网）及应用与数据支持（例如存取机密资料、汇款、支付、用户管理等）功能的风险类型。从信息安全的角度来看，应用应该在组织的特定脆弱性评估和应用安全需求范围内。安全性验证和应用认证遵循特定的安全要求，如安全设计、安全编码，安全操作。这些往往是应用安全标准目标的一部分。

因此，合规性是应用程序的安全性的一个重要方面，也是首席安全官们的职责所在，但不是唯一职责。应用安全的扩展安全领域也是CISO的职责。这些可以概括为（ GRC ）治理、风险及合规性。

- 从治理的角度，首席安全官们负责机构应用安全流程，角色和职责的制定并且管理软件开发人员，同时对软件开发人员进行软件安全培训和安全意识教育，如对信息安全人员/管理人员进行防御性编码和脆弱性风险管理的培训。

- 从风险管理的角度来看，CISO管理的风险还包括应用安全风险，如针对特定应用的威胁通过利用安全控制的空白以及应用程序的漏洞窃取用户机密数据的风险。

- 在CISO的安全域中，遵守法规和安全标准往往会得到该组织的执行管理层最多的关注。本指南的目的，是帮助CISO满足合规性要求，以及利用合规性要求作为投资应用安全的理由。对于一些组织来说，管理安全事故风险，如信用卡欺诈，窃取个人身份信息，侵犯知识产权和机密数据，这些安全事件会吸引大多数的行政管理层的注意力，特别是当该组织已被数据泄露的安全事故所影响时。

（贺新朋）

第一部分 投资应用安全的原因

在这个数字时代，国有和私营组织通过Web应用为越来越多的市民、客户、顾客和员工提供服务。通常，这些Web应用在互联网上提供“高可信服务”，其中包括承受高风险的业务功能。这些Web应用成为越来越多欺诈者和网络罪犯的目标。导致许多拒绝在线访问，数据泄露和网络欺诈等事件。

CISO们（CISOs）的职责是执行应用安全控制措施，以避免、缓解和减轻影响该组织实现其使命时可能存在的安全风险。这种不断变化的威胁形式进一步推动了组织对审计、法律和合规性的需求。首席安全官们必须为一个应用安全计划投资建立一个商业案例。这个商业案例应当作为安全威胁的对策映射到业务和必要的服务计划之上。行业安全的投入标准和定量风险计算可以为安全预算投资需求提供支持。

（胡晓斌）

第二部分 管理应用安全风险的准则

CISO（以下简称：首席安全官CISO）必须找出首要关注的安全问题。为了决策如何管理应用安全风险，首席安全官需要评估为修复已知弱点所采取的控制措施的成本效益。为了降低应用程序的风险等级，成本与效益的权衡是决定采用哪些安全控制措施的关键因素。首席安全官经常需要向决策层解释风险，说明一旦应用受到攻击、敏感数据被破坏时对业务造成的潜在影响。当存在以下三个风险要素时，安全风险就成为业务风险：

- 威胁的可能性
- 漏洞的暴露程度
- 资产价值

为了系统地考虑风险等级的排序，首席安全官可以参考《通用弱点评价体系V2》(CVSSv2)。为了定期地与业务管理部门沟通应用风险，首席安全官可以考虑提供“《安全威胁意识报告》（emerging cyber-threat awareness）”给业务

管理部门。

与企业高管沟通

首席安全官需要真正地从业务风险的全局去考虑信息安全风险。不仅是合规和安全弱点，也包括组织的信息资产相关的威胁、安全事件等安全态势。首席安全官清晰地将安全态势信息传递给决策层有助于说明对信息安全措施进行投入的价值。当然也需要将目前的成本与采取其他安全措施的成本，和一旦发生安全事件造成的损失进行比较。目前一旦发生安全事件所造成的损失要比合规性检查或审计没有通过的成本要大得多，往往安全事件会让首席安全官丢了自己的工作，同时影响到公司的声誉和效益。

威胁建模

通过自上向下的方法来识别威胁和控制措施，向首席安全官介绍需要考虑到的威胁建模技术（第三部分也会描述）。威胁建模技术将所需保护的应用进行分解，分析其攻击界面和面临的威胁，所采取的相关对策、差距及不足。

运用新技术

移动应用、Web2.0以及云计算服务这些新的应用技术和平台也引申出了新的威胁和防护技术。应用的变更也同样是风险源，尤其是当一些新的或不同的技术都集成在同一个应用中。随着应用的发展，新的服务被提供给用户、客户和雇员等更多的人，这就需要我们去关注和处置如移动设备、Web2.0等新技术和云计算等新的服务方式所带来的安全弱点。采用风险管理框架以评估新技术带来的风险是必不可少的，以确定采取哪些控制措施来降低这些新风险的等级。本指南将向首席安全官提供指引，以应对由新技术的采用所有带来的新的威胁、漏洞和风险。

- 移动应用
    - 风险举例：设备遗失或被窃、恶意软件、多路通信信道泄露、弱身份认证；

- 措施举例:制定移动安全标准，通过审计来评估移动应用中的弱点、安全配置以及个人设备中的应用数据。

- Web 2.0
  - 风险举例:社交媒体的安全、内容管理、第三方技术和服务的安全;
  - 措施举例: 安全API，验证码（CAPTCHA），在提交和交易确认过程中使用特殊的安全令牌。
- 云计算服务
  - 风险举例:多租户部署、云计算部署带来的安全问题、第三方风险、数据泄漏，来自内部恶意的拒绝服务攻击。
  - 措施举例: 云计算安全评估，对云计算供应商的合规性审计，人员尽职调查，存储和传输过程中的加密，监控.

目前的攻击者（威胁代理）更多是为了经济利益去攻击应用，以获取敏感数据和公司内部的信息，以及通过欺骗方式获得竞争优势信息（例如网络间谍），从而损害用户利益。为了降低这些攻击者（威胁代理）所带来的风险，有必要确认风险的接受水平、安全事件发生的可能性及影响、识别应用漏洞可能被利用的场景。这些弱点一旦被利用会对组织和业务造成严重影响。

（郝轶）

第三部分 应用安全计划

从整个风险管理策略来看，应用安全风险的缓解不是一次性的而是一项持续的活动，需要密切关注新出现的威胁，并规划和部署新的安全措施，以消减这些新威胁。包括规划采取新的应用安全活动、流程、控制措施和培训。在规划新的应用安全流程和控制措施时，对于首席安全官而言，为了实现业务使命，了解在哪个应用安全领域进行投资是非常重要的。

要建立和发展一个有效的应用安全计划，首席安全官们必须:

- 映射业务优先到安全优先

- 使用安全计划的能力成熟度模型评估当前的状态
- 使用安全计划的能力成熟度模型建立目标状态

映射业务优先到安全优先

所有的安全优先级必须能够映射业务重点。这是致力于建立所有安全倡议的重要性，并展示企业管理安全性如何支持业务的第一步。它还向安全人员演示了工作人员如何支持这种使命。

使用安全计划的成熟度模型评估目前的状态

访问过程成熟度是通过应用安全和软件安全过程的先决条件。常被组织采纳的标准之一是考虑组织在应用安全领域的能力和组织在这些领域操作的成熟度。

这些应用程序安全领域的例子包括应用安全治理、脆弱性风险管理、合规性和应用安全工程，如设计和实现安全的应用程序。特别是在应用安全工程的情况下，采用软件安全保障往往是必要的，而没有实施这类软件安全性，是因为它由第三方供应商直接控制生产。在这种情况下要考虑的一个因素是使用成熟度模型来衡量软件的安全保证。采用安全软件开发生命周期（S- SDLC）测量软件的安全保证是一个先决条件。在高级S- SDLC中包含软件开发生命周期内的培训和工具中“构建安全”的安全活动。这些活动的例子可能包括软件的安全流程/工具如构建风险分析/威胁建模，代码的安全性评价/静态源代码分析，应用安全测试/应用漏洞扫描和软件开发人员安全编码。OWASP软件保证成熟度模型，以及几个专用于软件安全的OWASP项目和S-SDLC和本指南都可以做为参考。

使用安全计划的成熟度模型建立目标状态

并非所有的组织都需要达到最高的成熟度。成熟度应该维持在一个能够管理影响业务的安全风险的水平。显然，这在不同的组织之间有所不同（变化），并且这和业务有关，以及能接受的作为来自安全组织的持续合作以及透明度的一部分的风险有关。

一旦目标状态是确定的，CISO应该建立一个确定其解决已知问题的战略，以及检测和减轻新的风险的路线图。

OWASP提供了几个项目和指南，来帮助CISO制定和实施应用安全计划。除了阅读本节中的指南，请参阅附录B：OWASP指南和项目高效参考，可以获得能够纳入应用安全计划的安全工程领域的活动类型的详细信息。

（贺新朋）

第四部分 管理风险及应用安全投资度量

一旦应用安全和软件安全投资建立，CISO来测量和报告应用安全计划在治理、风险和合规性执行管理的现状是非常重要的。此外，CISO需要证明应用安全计划投资及其对业务风险影响的有效性。

CISO还需要度量管理和监控人员、流程和技术，弥补应用安全计划。例如衡量治理，也包括风险和应用安全流程的合规性等指标。

安全度量分为三类：

- 应用安全过程度量
- 应用安全风险的度量
- 在软件开发生命周期的安全指标

应用安全过程度量

这些支持通过明智的决策来决定哪些地方需要集中的风险缓解工作和更有效地管理应用安全风险。

这些风险管理的目标通常是与组织有业务往来的特定组织和依赖于组织机构的类型和行业部门，以决定哪些应用安全风险应优先采取行动。

- 对组织适宜的安全政策，技术标准和行业惯例效果如何？
- 我们如何贯彻执行安全SLA？通过应用程序？部门还是渠道？

应用安全风险度量

- 脆弱性风险管理度量 - 什么是在年度基础上的平均修复时间？按月？按应用？按部门？有哪些过程存在已知的安全问题？
- 安全事件度量 - 哪些安全问题已经被利用？他们从哪里知道这些过程的问题？什么是业务成本？
- 威胁信息报告和攻击监控度量 - 哪些应用正在遭受比其他应用更多的攻击？哪些应用需要面对即将到来的预期峰值的使用？

软件开发生命周期的安全度量

一个经常被忽略的方面是花费在处理软件安全的经济效益往往是在不安全的软件应用之上。在软件安全方面的投资就其本身而言应是在软件发布之前识别和解决安全问题，这样可以节省企业的成本；因为应用被发布到生产环境后修补漏洞的成本是非常昂贵的。它比投资于安全架构评审，以识别和补救他们之前的编码设计缺陷，以及投资于安全代码审计过程中的编码来识别和修复软件安全漏洞，并确保发布的配置是否正确要便宜很多。

- 风险缓解决策度量 - 什么是应用风险类别平均修复时间？它是否达到预期？什么是应用程序的风险热图？按部门？按渠道？
- 脆弱性根源鉴别度量 - 每个应用脆弱性的根源是什么？是否是一个系统问题？哪项安全实践已经被每个开发团队很好的采用？哪个开发团队需要更多的关注？
- 软件安全投资的度量 – SDLC哪个阶段确定的安全问题最多？每个SDLC阶段相应的安全措施的成熟度是什么状态？在每个SDLC阶段安全人员、流程和技术什么是最迫切需要的？安全性测试与下游漏洞渗透测试哪一个更节约成本？在每个阶段所发现的问题节约的成本是什么？

（樊山）

CISO 指南

第一部分：投资应用安全原因

I-1 内容摘要

在这个数字时代，国有和私营组织通过Web应用为越来越多的市民、客户、顾客和员工提供服务。通常，这些Web应用在互联网上提供“高可信服务”，其中包括承受高风险的业务功能。这些Web应用成为越来越多欺诈者和网络罪犯的目标。导致许多拒绝在线访问，数据泄露和网络欺诈等事件。

CISO 们（CISOs）的职责是执行应用安全控制措施，以避免、缓解和减轻影响该组织实现其使命时可能存在的安全风险。这种不断变化的威胁形式进一步推动了组织对审计、法律和合规性的需求。首席安全官们必须为一个应用安全计划投资建立一个商业案例。这个商业案例应当作为安全威胁的对策映射到业务和必要的服务计划之上。行业安全的投入标准和定量风险计算可以为安全预算投资需求提供支持。

I-2 简介

应用的增长在组织中越来越重要。通常情况下提供关键服务的法律和监管要求。对于银行客户，这些功能丰富的功能，使他们能够开立银行账户，支付账单，申请贷款，图书资源和服务，转移资金，交易股票，查看账户信息，下载银行对账单等。这个在线体验是为了方便人们：他允许从他们的家用电脑或手机上在分支机构/办公室/出口远程便利的执行相同的金融交易。同时，方便客户所带来的是参与开发和维护这些应用的金融机构要付出代价。例如，网上银行和电子商务网站已成为欺诈者和网络罪犯的目标并且安全事件的受害人数日益增加。这些事件中的若干个可以导致拒绝在线访问、破坏数据和在线欺诈。

在数据泄漏事件情况下，通常来自欺诈者和网络罪犯涉及到应用的这些攻击，如SQL注入的出现危及应用数据库的存储和跨站点脚本执行恶意代码数据，如用户浏览器的恶意软件。这些攻击的目标是数据和处理这些数据的应用业务功能两

类。在网上银行应用的情况下，由黑客和恶意软件攻击的数据包括以上人士的个人资料、银行账户资料、信用卡和借记卡数据、网上认证如密码和PIN以及最后但并非最不重要的更改数据，在线转账的金融交易进行诈骗。Verizon公司2012年的数据泄露调查报告指出黑客和恶意软件最突出的攻击类型，产生在密码和凭据被盗，从而构成任何组织网上交易的重大威胁。

为了应付增加的针对应用程序事件，如通常由黑客和恶意软件造成的拒绝服务和数据泄露，首席信息安全官（CISO们）像首席信息官（CIO），法律顾问或首席财务总监（CFO）一样成为公司的高官建立和执行应用安全措施来管理组织应用安全风险。以金融机构为例，日益增加的应用威胁，如在线银行应用，挑战CISO强制其他应用安全控制和提高应用安全方面的投资，以应付日益增加的风险。

由于不断变化的环境威胁，从审计，法律及合规压力增加，在过去十年中，应用安全的投资一直在整体的信息安全和信息技术预算中所占比例越来越大。这一趋势还获取应用安全调查，如2009年OWASP安全支出基准项目报告，例如指出：“尽管经济不景气，超过四分之一的受访者预期在2009年应用安全支出预计增加36%。” 此外，在2013年OWASP的首席信息安全官调查显示，约87％的受访者表示应用安全投资将增加或保持不变。尽管如此，令今天增加应用安全预算的商业案例依然由于经济衰退和支出的优先顺位新的应用功能和平台（如移动设备）开发的一个挑战，以扩大服务的摄取或盈利能力和市场营销来吸引新客户，留住老客户的措施。最终，在当今经济不景气的环境类型和缓慢生长的业务投资，包括该公司内建软件的情况下，CISO们阐明投资与应用安全的“商业案例”越来越重要。由于它看起来是组织威胁认知（应用安全威胁是最大的）和花费在网络和基础设施的安全问题要高得多之间存在脱节，我们想阐明因应用漏洞攻击导致的组织数据泄露和对业务影响的多少产生的费用。通常情况下，额外的预算分配应用安全，包括更改应用程序来解决该事件的原因（如修复漏洞），以及推出了额外的安全措施，如减轻黑客和恶意软件的风险防范和控制探测的发展和限制未来数据泄露事故的可能性和影响。

CISO可以对由于今天不同的原因为应用安全追加预算而建立一个商业案例，一些直接针对特定公司的风险文化和风险偏好，另外定制应用安全需求。有些需求可以通过应用安全调查结果的分析来识别。为了评估这些需求，本指南邀请读

者参加OWASP的CISO调查，使本手册的内容可以针对参与调查的CISO的需求。

2013 CISO调查：关注成长

增加应用风险有针对性的威胁的感知和组织从传统的网络安全投入向应用安全转变。

应用安全预算以该公司的年度预算的比较

•47％CISO们都有所增加

•39％的人认为它相对稳定

•13％的人出现了下降

应用安全措施预算编制可能取决于不同的因素，如符合安全政策法规，操作风险管理，包括由于应用漏洞的风险和涉及应用安全事件的响应。对于本指南，我们将重点在以下领域的应用安全支出为目标。

- 安全标准、安全政策和法规符合；
- 识别和修复应用漏洞
- 实现针对应用新兴威胁的对策

然而，假设商业案例可以沿着这些目标进行，今天CISO们仍然有艰巨的任务，确定“多少”钱应该花在公司的应用安全和对“哪些安全措施”支出到“哪里”。至于多少钱，通常要根据需要投资多少可以将风险降到可接受程度已满足合规性要求，并通过审计师的检查。当焦点是合规时，重点是制定和执行应用安全标准并映射这些安全要求在当前项目。当焦点是安全事件管理时，重点是如何调查和分析可疑的安全漏洞和推荐纠正措施。当焦点是应用安全意识，重点是为在职人员申请应用安全培训。

今天对于CISO更加注重缓解风险的决策。减轻实际风险（例如事件、漏洞攻击）和违规风险（如违法违规）两个方面，对于CISO的问题是在“哪里”和“怎样”优先考虑应用安全预算的支出。通常情况下，问题是哪些对策、应用安全过程、活动或安全工具能够为组织“更直接的带来更多的钱”的收益。关于“在哪里”可以把它归结为正确地平衡不同应用安全和风险域-说出下面最重要的：企业治理、安全风险管理、运营管理，包括网络安全、身份管理、访问控制和事件管理。既然作为一门学科，应用安全包含了所有这些领域，必须从应用安全不同的角度考虑这些投资是非常重要的。

I-3 信息安全标准，政策和法规遵从

确定标准，政策和其他任务的范围的符合性

其中一个应用安全计划资金的主要因素是符合信息安全标准，政策和适用的行业标准监管机构授权的规定。最初，对于CISO重要的是定义合规性以及如何影响应用安全的范围是什么。

根据不同的行业部门和机构业务所在的地理位置，会有多种不同类型的组织需要遵守的安全要求。这些要求的影响还在于管理应用和过程数据的安全在这些标准和法规的范围之内下降。对应用的影响包括执行计划的风险评估，并就合规状况报告给审计师。

示例：适用于美国应用数据安全和隐私标准包括：

- 支付卡行业（PCI）数据安全标准（DSS）的支付卡商户和处理器
- 美国金融机构的应用允许客户和消费者使用网上银行业务，并进行诸如支付和转账交易FFIEC指南
- FISMA法律为美国联邦政府机构的系统和应用为他们的行动提供信息安全和资产需要
- HIPAA法律为保障美国的医疗保健行业病历隐私的健康数据的应用处理
- GLBA法对美国金融机构的申请收集和存储个人的个人财务信息
- 美国国务院数据违反信息披露法规的组织，他用于处理美国各州居民个人可识别信息（PII）数据明确在应用存储和处理这些数据丢失或被盗（例如未加密）
- 组织FTC隐私规则，其申请办理在美国的消费者私人信息，以及在欧盟国家工作时遵守“免责”规则

OWASP提供了一些项目和首席信息安全官指导，帮助制定和实施政策，标准和应用安全指导方针。请参考附录B： OWASP指南及项目的更多信息快速参考。

收集应用程序的安全要求

PCI DSS（第三方支付行业(支付卡行业 PCI DSS)数据安全标准）

大多数进行支付交易，例如电子商务应用处理信用卡持卡人数据商户类型的应用都必须遵守支付卡行数据安全标准 PCI DSS。对于持卡人由应用存储数据保护的要求，PCI DSS 要求如呈现或加密主帐号（PAN）时应该遮盖 PAN 的显示。PCI DSS 要求卡的身份验证数据，如密码，CVC2/CVV2/CIDs 不存储所有这些数据，即使是在授权付款后的加密表格。信用卡持卡人的数据在开放式网络传输时需要通过加密技术保护。保护持卡人的个人帐号和持卡人验证数据这些要求推动 CISO 以内部文件的方式要求遵守这些安全规定，并采取应用安全措施和评估，以确认这些要求都是满足由相应应用的范围。除了对持卡人信息保护外，PCI DSS 具有安全系统和应用开发和维护的规定，用于测试安全系统和流程以及对常见的漏洞应用测试，比如 OWASP Top 10 的定义。

通过在技术和应用安全检测服务的额外投资作为理由来证明符合 PCI DSS 规范的必要性：例如源代码安全审计与 SAST（静态分析安全测试）评估/工具和应用安全审计与 DAST（动态分析安全测试）的评估。对于一个商人，开发和维护一个 Web 应用，如用于处理信用卡支付的电子商务网站，主要的问题是，是否给应用安全对策和活动分配预算，以符合 PCI DSS 或承担罚款（如信用卡持卡人数据丢失或被盗达到$500，000）。从这个角度来看，违反法规和标准的合规性可能和其他任何风险一样被视为组织的另一种风险，可以减轻、转移或接受。如果不合规风险被接受，CISO 应该考虑到数据泄露的风险，因为没有执行基本的安全控制，如数据加密，还要输入验证，可能会比不合规的风险要高得多。

例如：T. J.MAXX 违反 PCI DSS。

T. J.MAXX 违反 PCI DSS 导致 94 万个信用卡号码数据被泄露。然而，因未加密或者卡号被截取并修复应用漏洞的违规成本，如 SQL 注入，较少产生的安全事件影响了企业的整体成本。在 T. J.MAXX 信用卡数据泄露事件的案例中，T.J.Maxx 因为事件产生的经济损失至少要比由于没有遵守 PCI DSS 所造成的损失高出一千倍（甚至更多）：相当于数亿美元和数万美元的比较。

FFIEC（美国联邦金融机构研究委员会）

在美国银行业，处理敏感客户信息的应用和允许处理的金融交易如：以不同银行账户（例如：电子转账）之间转移资金，必须符合美国联邦金融机构检查委员会（FFIEC）网上认证指引。要求包括强认证等多因素认证（MFA）。

应用程序安全投资的业务驱动

联邦金融机构检查委员会（FFIEC）要求，对网上银行站点的身份验证要有充分的理由证明应用程序安全在安全设计、实施和应用测试方面提供MFA控制预算。

GLBA（格莱姆-布里勒法规）

对于美国消费者来说，隐私是在根据不同行业的法律和法规监管。在美国，金融部门，支配消费者隐私的法律包括GLBA法和联邦贸易委员会（FTC）规则。

从 GLBA 合规性的角度来看，金融应用需要提供披露其 PII 的收集，处理和存储以及它是如何在金融机构的业务和分支机构，包括第三方共享应用程序的用户。从美国联邦贸易委员会合规的角度来看，存储客户 PII 组织需要透露自己尽职调查安全实践给消费者并且可以为其承担责任时，这种做法没有遵循作为违反消费者的私人信息的情况下，并在一个明确的违反与消费者的许可协议。因为在美国的隐私法主要是要求承认消费者的个人数据受到保护，安全性的影响是有限的通知，确认和“退出”控制。例外的是，其中的隐私控制实现为应用的隐私设置（例如在 Facebook 上的情况下），并提供给用户的应用为“选择控件”，以符合美国联邦贸易委员会免责规则的情况。

隐私法

在一般情况下，应用需要保护存储和被认为是个人和私有的国家特定隐私法在这些数据在存储或处理时处理的数据。何为私人信息各个国家因国家情况而异。例如欧洲联盟（欧盟）的一部分国家，在欧盟指令95/46/EC中对个人数据的定义，该指令在第24条A“‘个人资料’指有关识别或可识别自然人（“数据主体”）

的任何信息；可识别的个人是一个谁可以被直接或间接地识别，特别是参照的识别号码或与一个或多个特定于他的物理，生理，心理，经济，文化或社会身份因素”。

对于美国大多数的国家，保护个人身份信息（PII）是由数据泄露通知法律驱动，如SB1386中的PII比欧盟指令更狭义的定义作为个人的名字或首字母和姓氏与以下任一数据或多个元素组合时，无论名称或数据元素是否被加密：（1）社会安全号码。（2）驾驶执照号码或州身份证号码。（3）户口号码、信用卡或借记卡号码，任何允许访问个人金融账户所需的安全码、接入码或密码的结合。出于法律的目的，“个人信息”不包括从联邦，州或当地政府记录公开资料被合法提供给广大市民的内容。

过程和存储数据应用由欧盟隐私法或美国国家数据泄露通知法PII对于个人隐私数据，需要实施安全控制，如身份验证，授权，加密，日志记录和审计，保护机密性，可用性和该数据的完整性。这些信息安全的要求通常是组织实施信息安全策略的一部分。这些安全要求间接转换存储和应用过程的数据被视为机密或者机密的PII数据安全要求。符合个人和消费者数据隐私要求的应用安全计划同时作为内部合规与信息安全政策，以及为数据丢失或泄露减轻受损组织的声誉的情况下编制预算。除了名誉受损，组织可能会招致因不遵守当地的隐私权法律法规的罚款和诉讼费用。

I-4 风险管理

风险管理一定是CISO的核心功能之一。本节指南的目的是帮助CISO开发、阐明和实施风险管理的流程。OWASP还为CISO提供了可用的文档指南实现对应用的风险管理策略。阅读本节之后，请参考附录B中的OWASP指南和项目参考。

主动式 VS 反应的风险管理

积极的风险管理包含专注于减轻威胁事件的风险之前，这些有可能会发生并造成负面影响的组织。组织重点是积极的风险管理，规划，保护关键任务资产，包括针对未来这些潜在威胁的应用。应用主动的风险缓解活动包括专注于威胁情报，以了解威胁代理，应用威胁建模，以便了解 应用如何可以通过不同威胁代

理攻击，安全性测试和应用中潜在的漏洞的加固，以及在这些源代码被潜在攻击着利用前进行保护。积极的风险管理的前提是的风险状况使CISO可以确定关键应用相关联的关键数字资产的清单，如数据和需要被优先考虑和计划主动降低风险的活动的功能。CISO专注于组织前瞻性的风险缓解措施，通常采纳威胁情报和监视安全事件和警报后信息的风险缓解策略和行动，以提高人们对可以接受的技术和业务风险水平线。CISO们重点是主动风险缓解措施通常需要推出在新威胁和新的合规性要求之外的附加对策。

反应性的风险管理包括应对风险事件发生时组织减轻负面影响。反应性风险管理活动的例子包括安全事件响应，安全事件调查和取证以及欺诈管理。在应用安全的情况下，反应性的风险管理活动包括漏洞补丁管理，修复应用漏洞响应报告的安全事故或当这些由第三方鉴定，，由于偶然的（没有计划）的要求执行应用风险评估，以满足特定的合规和审计要求。组织CISO专注于反应性的风险管理通常花费更多的精力放在应对意外的风险管理活动。通常翻译性风险管理的重点是“损害遏制”到“止血”，并不太注重致力于风险缓解之前针对未来应用潜在负面事件的规划。通常组织反应性风险管理的重点是CISO花费大部分时间在事件响应和管理修复应用漏洞无论是产品发布之前或者那些已经发布的生产应用的修补。当CISO认识到反应性风险缓解很重要时，他的职能首要的重点是反应性风险管理，即使它因为安全事故的发生而不能总是被避免，因为补救问题总是发生在报告或者已经被攻击者利用之后的几个因素的识别与通过预防性风险缓解措施相比并不符合成本效益。

在应用安全商业案例中最好的响应风险缓解的方法是积极主动的风险缓解。积极主动的风险缓解方法可能包括使用一个应用所需的技术升级，引入新的功能或当一个旧的应用生命周期结束时需要迁移到新的系统/平台的时机。设计应用的新功能表示 CISO 们需要升级安全技术新标准和执行更有利的安全措施以及机会。

资产为中心的风险管理

CISO的信息安全策略导出了符合信息安全标准，如ISO 17799/ISO 27001中包含的资产管理作为需要被覆盖的安全域之一。在这种情况下，这些资产包括应

用，组织为了实施风险管理办法进行管理应用资产管理需要的清单。这份清单包括的应用程序的类型信息，每个应用的风险，存储和处理数据的类型，修补要求和安全评估等所需漏洞测试。应用清单也很关键，跟踪应用安全评估和应用进行的风险管理流程已确认并修复，以及那些任然开放的漏洞得到补救。分配给每个应用的风险，也可以存储在应用程序清单工具：根据依赖数据分类和应用提供的功能的类型的应用的固有风险，它可以规划风险管理和现有漏洞的缓解的优先次序，以及规划未来的脆弱性评估和应用安全评估活动。应用安全活动采取资产为中心的风险管理其中一个优点是应用威胁建模。从架构角度来看，资产由几个部分组成，如应用服务器，应用软件，数据库和敏感信息。通过应用威胁建模，可以识别各资产的威胁和对策。

CISO 重点是资产风险管理，应考虑实施以应用威胁建模的积极应用安全和资产为中心的风险管理活动。

技术 Vs 业务风险管理

在决定如何减轻应用安全风险时权衡技术风险和商业风险之间的问题是很重要的。技术风险是一个应用无论是技术漏洞还是控制缺陷的风险被利用可能导致技术的影响，如丢失和泄露数据，服务器/主机损害，未经授权访问应用数据和功能，拒绝或服务中断的例子。技术风险可以衡量技术事件/原因造成的机密性、完整性和可用性的影响如确定应用安全评估脆弱性。这些技术风险的管理通常取决于该漏洞的类型以及赋予它的风险等级，也被称为漏洞的“严重程度”。该漏洞的严重性可以根据计算后的风险评分方法，如FIRST的CVSS，而漏洞的类型可以基于该漏洞属于如使用MITRE公司CWE组进行分类。CISO可以用脆弱性风险评级报告，如优先安排高风险的缓解，未来安排被评定为中等或低风险漏洞。在作出这一技术漏洞的风险管理决策时，CISO暂时不会考虑该漏洞对业务的经济影响，如在丢失或泄漏这种情况下漏洞影响的资产价值。

当资产价值考虑在确定该组织的影响业务风险管理时。这就要求技术风险与资产价值脆弱性量化风险的关联。风险可以被分解为资产被损害的可能性及造成漏洞的攻击对业务的影响。例如，在这种情况下，高风险的技术漏洞，如SQL注入（假设完全是100%公开的作为预身份验证问题）被利用，对业务的影响可以

被确定为影响到的资产，如数据，已被列为敏感数据，且如果泄露导致的损害估计为$250/数据记录（例如基于无论是内部事件成本预算或公开报告的预算）的影响。因此，存储在数据库中的10万条记录可以通过SQL注入被利用导致敏感数据泄露的合计值是2500万美元。如果由于SQL注入漏洞攻击导致敏感数据泄露的概率为10%（每十年SQL注入会引起一次成功的数据泄露事件）的潜在经济影响是250万美元的损失。根据这些估计，就可以计算出在应用安全措施（如检测性和预防性控制）用多少预算缓解业务风险。

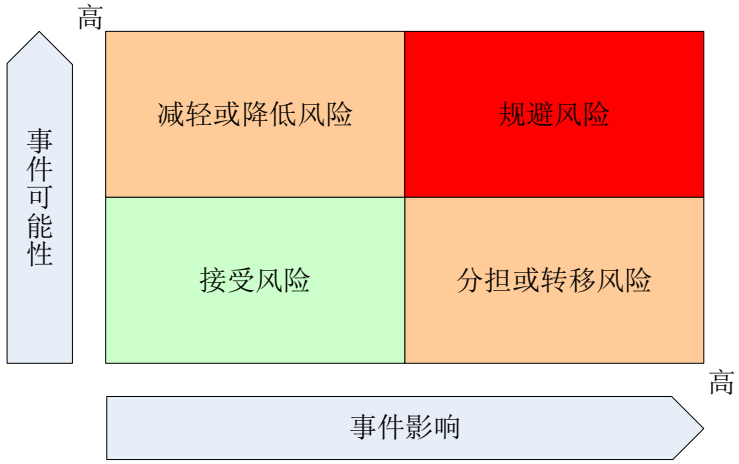
应该注意的是，评估业务风险比评估技术风险更加困难，因为业务风险评估需要特定类型的安全事件（如数据破坏）的可能性的评估以及事故造成的金钱损失（如收入损失、法律、合规成本、事故原因导致的维修成本）。通常，这些估算是难以在缺乏具体的数据和安全数据泄露事件的频率和保持该组织遭受这些安全事件导致的直接和间接成本的记录为因子的计算工具。

尽管如此，数据泄露事件的统计数据，数据破坏事件的费用估算以及数据泄露定量风险计算的可能。在附录A变量数据和一个事件的成本提供范例中，公式和在线计算帮助CISO赋予信息资产货币价值，并确定该组织因安全事故导致资产丢失的情况下的货币损失。这些定量风险计算的目的是帮助CISO决定花费在应用安全措施的费用多少是合理的，以减少组织数据泄露事件情况下对业务的影响。

风险管理策略

一旦安全风险已经确定，并分配一个定性的值，如高，中，低风险，对于CISO的下一个步骤是确定如何处置风险。要决定“如何处置的风险”CISO通常依赖他们的组织的风险管理流程和风险缓解策略。风险管理流程在每种类型的组织中通常是不同的。高水平的风险管理取决于所采用的组织的风险缓解策略。取决于风险的影响和概率的高低进行评估，例如，一个组织可能觉得接受可能性和影响都很低的风险，减轻或减少具有高概率和低冲击的风险（例如，通过应用安全的措施），通过转嫁或共同分担低概率高影响（如与第三方通过合同协议方式）的风险，规避高概率和高影响的风险（如，不执行高风险的功能，不采用高风险的技术）。这种风险缓解策略，事件可能性和影响因素的情况如下图所示。

图 1 基于事件的可能性和影响的风险缓解策略



在高风险无法避免的情况下，因为业务决策需要减轻他们但风险无法通过合同协议和网络保险转嫁给第三方，该组织可能的风险策略可以减轻所属的中，高和可接受风险（如什么都不做），其残余风险（例如任何措施或补偿控制后留下的风险正在应用或考虑）只有低风险。风险缓解策略也可以采用定性风险分析的业务风险因素的风险因子如概率和经济的影响。一旦风险已经确定，下一步就是决定哪些风险组织愿意接受、减轻、转移或避免。对于组织是否愿意接受风险是很重要的，CISO有一个风险接受的过程，根据补偿性控制的出现他和行政管理人员在符合低风险水平时进行签字。对于被选择减轻风险的风险，确定哪些安全措施/纠正措施被组织视为可接受的，并决定哪些通过最小化成本最有效的降低风险措施是很重要的（如最大利益与最低保障措施的总成本）。这就是风险缓解策略需要考虑潜在的安全事件，如数据破坏的成本，来决定为组织预算中应用的安全性措施的投资多少是合理的。对于CISO的风险战略的一个重要方面，就是要决定哪些安全措施效果最好一起“万众一心”，包括采用预防性和检测控件来提供应用程序的资产的深度防御。最后，无论是否转让或与第三方共享风险，CISO重要的是通过法律确保组织与第三方服务提供商/法人签署的法律协议和服务许可协议记录风险责任条款。

威胁分析和新兴威胁的认知

不从新兴威胁和需要得到缓解风险的水平提高的影响分析风险数据使商业案例对应用安全的措施增加开支并不总是合理。威胁分析数据使风险管理决策明

智。如果没有这样的数据，管理层只剩下关于威胁的主观因素。

关于威胁的主观因素最常见的是基于恐惧，不确定和怀疑（FUD）的决定。作用在FUD以减轻由新兴威胁造成的风险是迟来的和无效的。根据FUD示例行动包括，但不限于：

- 数据泄露的恐惧
- 失败审计和法规遵从的恐惧
- 业务方面不确定的威胁
- 鉴于最近的安全事件对现有保安措施的有效性的疑惑

这部分指南的目的，是帮助首席信息安全官创建一个额外的商业案例应用安全投资基础而非建立在主观的因素在客观条件的威胁分析。从符合标准的角度来看，客观的考虑是基于一个理由投资于应用安全，其中包括影响应用的新安全标准和法规的遵守。从威胁分析的角度来看，客观的数据因素有关新兴威胁代理为获取经济利益寻求危及业务的影响。特别是关于制定风险减缓的案例中，有必要对CISO在避免假设和备份的情况下使用数据，例如报告和分析网络威胁和安全事件，数据破坏的成本基于概率和评估影响的责任和风险的定量计算来估算。基于风险的计算和数据泄露成本的估计，有可能为CISO阐明组织应该投资多少在应用安全并确定在哪些具体措施进行投资。

从畏惧的角度来看待这些事实，无论这个事件是正面的还是负面的，CISO也可以利用这种势头，而这是一种反应性风险管理方法和低成熟处理风险的一部分。

通常应用安全支出可以由负面事件如出现安全事故来触发，因为它会改变高级管理人员对于风险的看法。然而，CISO在2013年OWASP的CISO调查中应当可以发现推动安全投资需要用1至两年的时间路线图会更有效。

图 2 分析表明支持取得适当的安全投资为 1-2 年的路线图，请勿做较短和较长的路线图

（OWASP CISO 2013 年调查）

安全投资	3 个月	6 个月	1 年	2 年	3 年	5 年+	总计
减少	1.69%	3.39%	5.08%	1.69%	3.39%	3.39%	18.64%
增加的总支出%	3.39%	1.69%	18.64%	16.95%	3.39%	0.00%	44.07%
相对稳定	5.08%	3.39%	11.86%	10.17%	3.39%	3.39%	37.29%
累计	10.17%	8.47%	35.59%	28.81%	10.17%	6.78%	100.00%

在这种情况下，可能这笔钱已经被花费在降低损失，如果要补救这一事件并采取额外措施。主要的问题是在应用安全进一步投资会减少另一个发生在未来的类似的事件可能性和影响。一种方法是把重点放在有可能成为未来攻击目标的应用。

发生安全事故后解决业务问题

安全事件响应过程的执行情况对于每一个CISO而言是重要的。这样的安全事件响应过程需要一个安全问题识别的联系点，通过安全问题披露流程以及建立一个非正式的安全响应团队。在发生安全事故的情况下，首席信息安全官通常负责进行事故根源分析，收集每一事件度量和建议的纠正措施。在附录B中，我们提供一个OWASP指南和项目快速参考给CISO，帮助首席信息安全官调查和分析疑似和实际应用的安全事故和建议的纠正措施。

一旦事件发生的根源已经查明并且已经采取行动纠正并遏制安全事故带来的影响，CISO的主要问题是应该怎样做才能防止类似的事故在未来再次发生。如果应用已经被针对性攻击和敏感数据丢失或受损，应用和软件的主要问题是是否今后可能再发生类型的攻击和事故的风险。由于恶意软件和黑客攻击由组织开发和管理的应用和软件，对于CISO的主要问题是应用安全措施和活动应有针对性的支出，以减轻破坏敏感数据的风险。

这些措施选定后，接下来的问题是应该在这些对策上花费多少。从成本和利益的角度来看，应用安全支出匹配所有的可能的数据泄露的业务影响的成本是没有道理的，因为它会令企业投资更多的在没有风险利益的对策，从而无所作为。因此，对于CISO的主要问题是应该花多少以减少由于一部份数据泄露事件的风险导致的实施安全措施的支出。如果不是100％，是50％，25％，或所有可能的金钱损失10％？另外，我如何估算出现安全事故的经济损失？我应该使用哪种方法？损失估算是否包括非金钱损失，如名誉损失？

该指南以下部分的目标是通过分析数据泄露事件的风险，货币化经济影响及估算可能性和业务影响减轻数据泄露事件风险，帮助CISO建立应用安全措施预算。只有在这种“风险尽职调查”的工作已经完成，才有可能确定成本和风险缓解效益对比，并决定在其保安措施进行投资。在本指南的附录A中，我们提供一

个信息资产货币价值赋值的快速参考，并确定基于统计数据的安全事件的财务影响。实施措施后，测量和监测安全性和风险是很重要的。在附录B中，我们提供的OWASP项目，可以帮助首席信息安全官组织内测量和监控安全和应用资产的风险的例子。

减轻数据泄露事件风险的应用程序的安全性措施的预算编制

首席安全官（CISOs）指南做出决策“组织在应用安全上需要投入多少钱的预算” 。我们将专注风险缓解准则，而不是其他因素，如：整体信息技术比例（IT）预算和去年同期相比的预算分配，应用安全作为整个信息安全预算的一部分。包括合规和运营管理成本。本指南中提到基于风险的应用安全预算准则包括以下内容：

- 评估一个安全事件发生时所产生的影响的成本
- 定量风险评估每年因为安全事故损失的费用
- 优化涉及事件成本和安全措施成本的安全成本
- 应用安全措施的安全投资回报

我们将在本指南的以下部分解释上述每一项标准，以及他们怎样量化应用安全措施的费用。

分析数据泄露事件的风险

确定安全事件风险的两个重要因素：事件所造成的安全事件的负面影响和可能性（概率）。要获得一个安全事件产生时影响成本的评价，关键因素是有能力确定安全事件产生的成本。由于安全事故对组织产生负面影响的例子可能包括：

- 名誉损失，例如上市公司被公布安全漏洞后导致股票价格下跌的后果的情况；
- 收入，如针对客户的销售服务或商业网站拒绝服务导致的损失的情况；
- 公司数据资产丢失，如用户的机密数据、个人身份信息（PII）、认证数据和交易秘密/知识产权数据；
- 无法为广大市民提供法定的服务
- 已经曝光的个人数据造成的不利影响

数据泄露事件带来的货币化的经济影响

安全事件造成敏感客户或员工数据丢失的情况下，如个人身份信息，借记卡和信用卡数据，招致该组织遭受损失的成本包括若干运营成本也被称为故障成本。对于一个金融服务公司而言，更改帐户号码，签发新的信用卡和借记卡，因为欺诈者利用窃取的数据进行非法支付交易，以及自动柜员机提取款项时承诺提供预防欺诈的责任成本等，这些都是缓解成本费用。很多时候，这种“失败”成本的确定不是由组织直接量化的，例如当这个安全事件并不直接导致金钱损失时，应被推定为可能产生的影响。在这种情况下，CISO可以使用统计数据来确定这种情况下的数据丢失事件对公司可能的责任成本。通过使用从数据丢失事件报告的统计数据，有可能估算由公司引起安全事件修复所产生的损害以及导致敏感数据或同一性损失的损失成本。

数据的价值在每个组织不同，但记录值在 500-2000 范围内似乎是共同的。

数据价值：每记录$200 to $2,000

我们将在余下的讨论中使用这个范围，但每个CISO需要想出他们自己的一些评估，然后可以用来计算数据丢失产生的影响。

注：附录A包含了数据和事件成本价值的详细讨论，评估数据泄露的基于统计数据成本的实例和数据泄露计算工具。

预测数据泄露事件的可能性

对于公司来讲，其中一个挑战是计算因为一个潜在的数据丢失所导致丢失受害者的数量和对这种损失发生的概率或可能性的准确估计。有关发送到负责收集美国各司法管辖区的攻破通知信的开放信息安全基金会（OSF）DataLossDB的数据丢失事件的统计报告数据显示，2010年的数据丢失事件攻破一个web界面的比例为9％，而作为一次黑客攻击的百分比是12％，诈骗10％和病毒2％。比例最高的类型是笔记本电脑被盗，占所有报告事故的13％。

从OSF DataLossDB相关网页获得的数据与从Verizon的2011数据外泄调查的统计数据的数据报告不同，其中黑客攻击（如蛮力，凭证猜测）和恶意软件（如后门程序，键盘记录器/形式采集卡，间谍软件）代表大多数安全突破（分别为50％和49％）和针对应用程序的攻击占所有的攻击媒介的22％和38％。

这些差异可以由以下事实来解释，Verizon根据美国特情局数据的一个子集的研究，不包括例如涉及盗窃和诈骗的计算，而不是对整个OSF DataLoss数据库的统计数据。此外，根据Verizon的报告;“调查的范围被缩小到只有那些涉及确定数据泄露的组织”。在OSF的情况下，调查数据除了包括美国国务院的数据泄露通知法导致泄露客户的个人身份信息（PII），还包括报告与发送到美国各个司法管辖区的事件。

量化数据泄露事件对业务的影响

在该情况下，当发生因安全事故造成的数据泄露的影响没有被记录下来，需要根据风险评估来估计计算，在遵守不同国家和地区执行的数据泄露通知法情况下通知公众。除了为基于数据的值负债成本的计算（请参阅附录的数据和一个事件的估计数据的价值成本的值），定量风险分析可以通过计算安全事件每年造成的影响作为依据来估计年度应用程序的安全性措施的开支。定量风险可以通过单一预期损失（ SLE）或概率的评估来计算的安全事件和发生的年率（ ARO ）或安全事故的发生频率的结果。通过定量风险分析，并采用公开发表数据泄露的报告，首席信息安全官可以估计一个给定的组织由于一个应用程序漏洞被利用而带来的损失，因此应该把钱花在应用安全措施上，以减轻数据丢失的风险。这种风险估计的准确性取决于数据泄露事件有多可靠和与应用安全的相关性。因此，重要的是要仔细选择数据，因为这是被报告为由应用程序的漏洞攻击造成的，如SQL注入（例如索尼和TJX公司最大的数据泄露）的攻击。

SLE可以用下面的计算公式:

SLE = AV x EF

其中，AV是资产价值（AV），EF是暴露因子（EF）。EF代表了资产损失的百分比，因为实现的威胁或事件。在2003年美国联邦贸易委员会（FTC）事故数据的情况下，这表示遭受身份欺诈的人口的数量达到4.6％。

假设6.55亿美元100万账户（根据2003联邦贸易委员会的数据655美元每个账户）的AV和4.6％的风险系数，数据泄露事件的估计SLE是30130000美元。假设攻击频率每5年1次，如在TJX公司数据泄漏事件（发现于2006年十二月中旬，并且由于SQL注入攻击）的ARO为20％的情况下。因此，估计每年损失或年预期损失（ALE）

可以用以下公式计算：

ALE = ARO x SLO

因此，计算出的数据丢失事件在 10 年内的年预期损失（ALE）是 6026000 美元/年。

在进行投资之前，考虑到成本和应用安全措施效益

现在的问题是，采用定量风险分析是否能得到对应用安全性措施的最优投资的估计。诚实的回答是，不一定。正确的答案是使用成本与效益分析，以确定最佳值。通过比较安全事件的成本与安保措施的成本，以确定最大化的收益是可能的，即应用程序的整体安全性。

在以软件安全成本为例的情况下，如图1所示，由于软件安全性的故障，包括安全事件的成本下降，同时该公司在在安全措施上花费更多的钱。这里的假设是，在安全措施上增加投资相当于减少风险，并为企业减少影响。这是基于当安全投资增加而风险下降的假设。另一个假设是，投资是用于有效的降低风险的安全措施。决定哪些安全措施能有效的缓解风险和应该被投资，它暗示着首席信息安全官都做了风险分析，并且找出最具成本效益的安全措施（如流程，技术控制，工具，培训和宣传等），并选定那些降低风险最多，实现起来成本最低的措施来部署和维护。注意：这个可能并不总是如此，因为在安全措施方面的支出并不总是转化为风险缓释增加：例如反病毒保护花费更多不会减少恶意软件因为恶意软件被设计以逃避病毒特征码检测系统。

在决定是否值得投资之前，最重要的事情是要考虑安全措施在缓解特定威胁所可能带来的影响的有效性。我们在本指南的第二部分提供指导，以帮助首席信息安全官识别哪些漏洞应优先修复，确定哪些安全措施能最有效缓解针对Web应用的特定威胁。在作出投资哪些安全措施之前，请参照第二部分“用于管理应用安全风险的标准”。

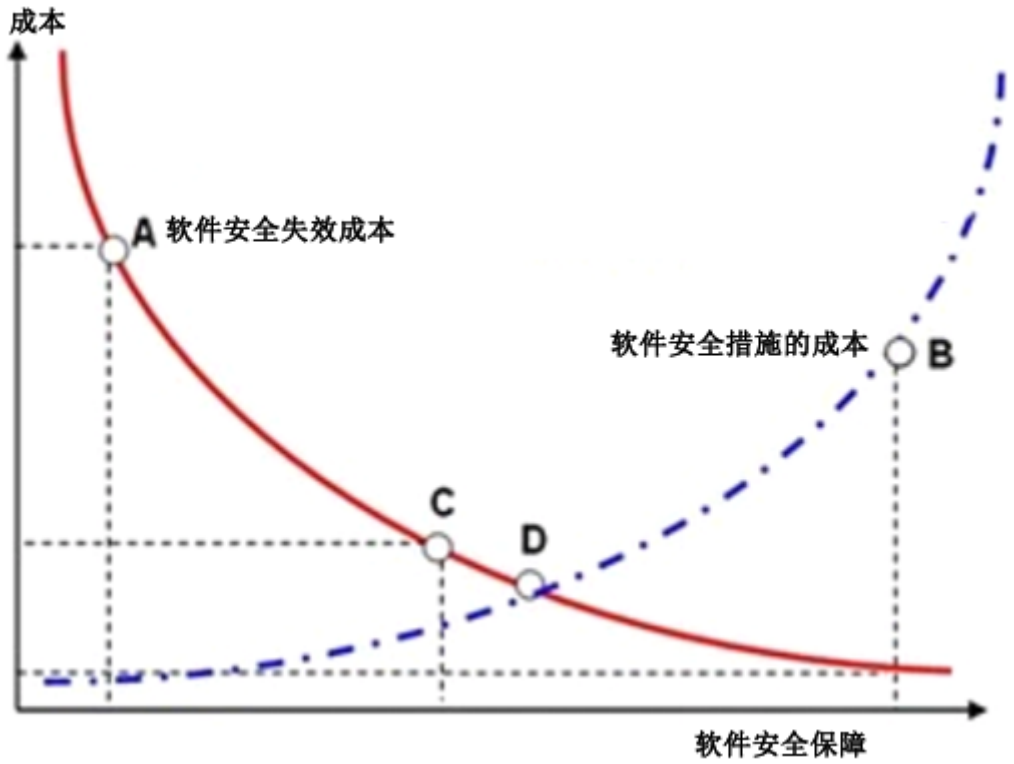
有了这些假设，将更多的钱用在安全措施上，以防止安全事故，在安全事故发生时损失更少的钱，如从安全事件中恢复成本，修复系统漏洞，实施新的措施和支付监管罚款，合同责任成本及法律费用。这里的假设是因为在保护和检测的安全控制，检测和修复漏洞，以及其他措施方面增加支出，安全事故将不太可能

发生，或者发生时将会减少对组织的影响。在应用程序的情况下，保障措施的实施属于应用安全计划的范围之内。首席信息安全官们可以参考本指南第三部分“应用安全计划”以了解其安全流程，工具和培训等这些首先应该被考虑进行投资的应用安全措施。

有了这些前提条件，随着越来越多的钱花费在应用安全上，直到成本大于收益的临界点。这显然不是风险管理的目标，如果可能不应该达到这个极限，因为这将破坏整个风险缓解策略，并会给首席信息安全官们压力，来辩解他们的预算。一个健全的风险缓解策略是一个要确定在哪个安全值进行投资给企业带来最大化的收益同时影响减至最低。这个值是投资的安全性措施的最佳值，这个值可以通过测量因为安全事故的发生的费用以及在安全措施的投资进行估算。假设该组织已经采用该成本度量标准，将有可能可以确定是否增加预算在减轻风险与减少安全事故数量和减少这些安全事故引起的整体影响。在本指南第四部分，我们为首席信息安全官提供关于“度量风险管理和应用安全性的投资”指导。在没有这样的指标来确定应用程序的安全性投资的最优值， CISO们可以看看关于最优投资点是当安全措施的成本估计是损失的37％的调查研究。对于我们的例子中，假设数据丢失事件造成的损失的总估计为6026000美元/年，对安全措施的最佳费用，使用这个研究的经验值，是2229620美元/年。

在下面图中的点（A），由于软件安全故障成本超过对策的开支的几个量级和对软件的安全性的保证是非常低的，相反在（B）由于安全措施的费用大于软件故障的费用，该软件可以被认为是非常安全的，但太多的钱花在软件安全保证上面。在点（C）损失的成本是安全措施近两倍的成本，同时在点（D）发生的事故成本等于安全措施的成本。对于安全措施支出的最佳值是1，能够最大限度地减少事故和减少安全措施的成本，并且能够带来最大化的收益或软件的安全性。

图 3 图表说明如何利用软件漏洞事故成本针对软件安全措施失效成本投资



分析安全措施投资

对于大多数组织而言，今天应用安全被没有被看作一种投资，但仍然是作为必然要实现符合标准和法规的成本投入。有些组织可能认为因为应用安全是风险管理要求的投入，其他人的认识是因为网络犯罪、欺诈和黑客主义者的威胁导致了暴露为理由。有些组织可能会考虑节省成本，投资安全提供了更短的“上市时间”，因为它们早于竞争对手发布安全的产品。也有些组织可能会意识到，在安全Web应用的花费可能增加用户在Web应用中可信度的级别，他们习惯于使用帮助保留这些客户业务以及出售更多的服务：这些组织可能会看到花费在应用安全的投资是一个积极的行为而不是成本。对于考虑安全性是投资而不是成本的组织，很重要的是确定花费在应用安全预算是从投资角度来看最有效的方法是什么。如果CISO考虑应用安全消费是作为一种投资而不是开支，例如，预算可能是因为公司在处理安全事故更少的花费作为额外的合理节约。

这是“省钱思维”的一个例子：“如果我再未来两年里为了防止安全事故一共花费了$$在保安措施上，在未来两年修复因安全漏洞所造成的安全事故的直接费用和间接费用估计的数字是多少。”一个计算在安全方面节约投资的方法是安

全投资收益（ROSI）。ROSI的使用可以帮助CISO们确定阻止特定网络攻击的对策的投资作为一项长期的安全投资是正确的：如果ROSI不是有效的，投资就没有意义，而如果是这无效的，它不会产生任何节约或投资回报。

有几种计算ROSI的经验公式；一种是避免总成本超过安全控制/措施中数据损失的成本的因素。假定安全控制/措施的总成本（TCO）费用是$2,229,620 （先前计算的每年消减SQL注入的安全控制费用的最优值），这包括开发成本及收购新技术，流程，工具以及运行和维护成本，就可以计算出节约的安全事故成本。ROSI可以使用下面的经验公式计算：

ROSI=[（ALE×控制效果%）- 控制成本] / 控制成本

有了这个ROSI公式，假设预先计算利用SQL注入漏洞造成的安全事故的ALE（年度预期损失）是$6,026,000.00，风险控制消减的有效性为75%，（例如：假定在SQL注入的情况下，风险消减的纵深防御，如监控，包括使用预处理语句/源代码存储过程，以及在Web服务器和应用服务器的不同层过滤恶意字符），安全控制的成本$2,229,620.00，该公司的ROSI是每年102%。安全投资收益这个值在安全控制措施支出是有价值的，他使公司每年节约资金。ROSI的最佳用途是在安全措施对比其他投资，如决定是否投资于新对策开发还是延伸现有的能力。

一个比较测量的例子，ROSI可用于CISO确定哪些应用安全的过程更加有效或者在组织软件开发生命周期（SDLC）过程中获得更高的回报投资和节省。据Soo Hoo（IBM）的研究，ROSI在软件开发生命周期的各种安全活动中，投资回报最高（21%）（例如在安全软件开发生命周期（S-SDLC）计划投资$100万，节省$21万）是当大部分资金投资于能够识别并允许在SDLC的设计阶段如建筑风险分析和应用威胁建模，以修复安全缺陷的活动。在SDLC的实现（代码）阶段的过程中发现如源代码分析缺陷并加以纠正时，甚至更低（12%）；当这些都在SDLC的测试验证阶段，如道德黑客/渗透测试，发现并加以纠正投资回报率较低（15%）。

通过使用 ROSI 作为 SSDLC 对比度量标准以最具成本效益的投资活动，因而在应用安全是能够尽可能早地识别缺陷活动，如需求和 SDLC 的设计阶段。本质上，CISO 们考虑投资应用安全计划，尤其是安全需求工程活动，如威胁建模/架构风险分析活动和安全代码审计，可以更多的节省实施和修复安全问题与其他活动的费用，如渗透测试。

结论

最后要注意的是，更好的使用涉及本指南中的风险和成本经验公式的成本估计所使用的数据值的可靠性是非常重要的。数据值越精确成本估算也就越准确。然而当这些风险成本的标准统一使用并根据测试的量化风险和可靠的数据，CISO 可以进行客观的风险和成本考虑以决定是否在应用安全措施的投资是经济合理的。这些风险和成本的考虑也可用于由 CISO 从哪些方面考虑坚持他们的预算并根据成本消减措施或要求更多的预算。今天，Web 应用所引起的风险和经济损失造成的安全事故增加了曝光率，以此为增加预算的理由是合理的。由于投资应用安全在业务方面是合理的，这些风险成本的标准可以用于商业案例，以及决定要花多少钱并在应用安全措施的哪些地方使用。

（陈亮）

第二部分：管理应用安全风险的准则

II-1 内容摘要

应用安全的利益相关者中，CISO（CISO）负责从治理、合规性和风险的角度考虑应用安全性。本指南旨在帮助CISO，根据CISO的角色、职责、观点和需要来管理应用安全计划。本指南中引用了应用安全最佳实践和OWASP的资源。OWASP是一个非赢利组织，其宗旨是“使应用程序的安全可见，并赋予应用安全与利益相关者正确的信息，用于管理应用程序的安全风险”

本指南可帮助 CISO，从信息安全和风险管理的角度管理应用安全计划。从信息安全的角度来看，对组织的资产进行保护是很有必要的，这些资产包括公民、客户端和客户敏感数据，存储这些数据的数据库,数据库服务器所在的基础设施，以及最后也是最重要的用于访问和处理这些数据的应用和软件。除了业务和用户数据，应用程序和软件也是 CISO 要保护的资产。其中一些应用程序和软件为组织产生了收益并为客户提供关键业务功能。例如，为客户提供商务服务以及应用和软件，给客户销售产品的应用和软件。在软件应用被认为是业务关键信息资产的情况下，这些应该在人力资源、培训、流程、标准和工具中得到特别的关注。本指南的范围是 Web 应用安全和结构与组件的安全，如 Web 服务器，应用服务器和数据库的安全；这不包括其他不相关的具体应用的安全。例如，支撑应用和构成一个有价值的资产的网络基础设施的安全属性，如保密性，完整性和可用性同样需要得到保护。

与企业高管沟通

首席安全官需要真正地从业务风险的全局去考虑信息安全风险。不仅是合规性和安全弱点，也包括与组织的信息资产相关的威胁、安全事件等安全态势。首席安全官清晰地将安全态势信息传递给决策层有助于说明对信息安全措施进行成本投入的价值。当然也需要将目前的成本与采取其他安全措施的成本，和一旦发生安全事件造成的损失进行比较。目前一旦发生安全事件所造成的损失要比合规性检查或审计没有通过的成本要大得多，往往安全事件会让首席安全官丢了自

己的工作，同时影响到公司的声誉和收入。

威胁建模

通过自上向下的方法来识别威胁和控制措施，向首席安全官介绍了需要考虑到的威胁建模技术（第三部分也会描述）。威胁建模技术将所需保护的应用进行分解，分析其攻击界面和面临的威胁，以及所采取的相关对策、差距及不足。

应用新技术的风险

移动应用、Web2.0以及云计算服务这些新的应用技术和平台也引申出了新的威胁和防护技术。应用的变更也同样是风险源，尤其是当一些新的或不同的技术都集成在同一个应用中。随着应用的发展，新的服务被提供给用户、客户和雇员等更多的人，这就需要我们去关注和处置如移动设备、Web2.0等新技术和云计算等新的服务方式所带来的安全弱点。采用风险管理框架以评估新技术带来的风险是必不可少的，以确定采取哪些控制措施来降低这些新风险的等级。本指南将向首席安全官提供指引，以应对由新技术的采用所有带来的新的威胁、漏洞和风险。

- 移动应用
  - 风险举例：设备遗失或被窃、恶意软件、多路通信信道泄露、弱身份认证；
  - 措施举例:制定移动安全标准，通过审计评估移动应用中的弱点、安全配置以及个人设备中的应用数据。
- Web 2.0
  - 风险举例:社交媒体的安全、内容管理、第三方技术和服务的安全；
  - 措施举例：安全API，验证码（CAPTCHA），在提交和交易确认过程中使用特殊的安全令牌。
- 云计算服务
  - 风险举例:多租户部署、云计算部署带来的安全问题、第三方风险、

数据泄漏，以及来自内部恶意的拒绝服务攻击

- 措施举例：云计算安全评估，对云计算供应商的合规性审计，人员尽职调查，存储和传输过程中的加密，监控.

目前的攻击者（威胁代理）更多是为了经济利益去攻击应用，以获取敏感数据和公司内部的信息，以及通过欺骗方式获得竞争优势信息（例如网络间谍），从而损害用户利益。为了降低这些攻击者（威胁代理）所带来的风险，有必要确认风险的接受水平、安全事件发生的可能性及影响、识别应用漏洞可能被利用的场景。这些弱点一旦被利用会对组织和业务造成严重影响。

II-2 简介

应用遭受网络攻击而导致数据泄露或者欺诈等安全事件，首要是要查清导致这些安全事件的根本原因（例如：漏洞、控制缺陷等）,然后投资建设安全防御措施，以防止类似安全事件再次发生。本章节中，我们将讨论如何构建安全的应用从而减少漏洞和风险。作为最佳实践，我们并不主张只修复漏洞，尽管这些漏洞是导致安全事件的起因，并且都应当在第一时间修复以阻止进一步的损失。已被利用的漏洞在未来可被重复利用的概率更高。

CISO 应特别关注：“未来，相同的漏洞是否可被用于攻击具有相似的功能和数据类型的应用?”。然而，应用可能还有其他类型的漏洞可能会被攻击者利用。这些漏洞之所以为能被用于攻击应用，是在于他们存在导致数据泄露和网络欺诈的风险。漏洞利用的可能性和影响是建设安全防御措施的重要考虑因素之一。总之，漏洞应基于技术风险而不是业务影响进行优先级分类，具有较高技术风险的漏洞应优先修复。SQL 注入就是一种典型的高技术风险漏洞。针对认证信息或者机密数据的 SQL 注入攻击相较于针对组织市场研究数据的会产生更严重的后果，后者所可能产生的风险是对组织声誉的影响，而不是数据泄露的风险。

本指南第一部分介绍了一些用于编列应用安全预算的商业案例。应用安全预算通常需要覆盖以下几点信息安全和风险治理的需求：用于信息安全标准、政策和法规的合规性要求的预算，和用于缓解数据泄露风险的预算。量化数据泄露事件发生的影响是编列缓解数据泄露事件风险预算的关键因素之一。这意味着

CISO 们需要授权访问与数据泄露事件相关的数据，包括有由安全事件应急响应小组（SIRT）提交的安全事件报告，与法律诉讼和监管有关的法律文件，以及因网络欺诈导致财务损失的欺诈数据。所有这些信息用于评估因数据泄露事件而产生的影响。在缺少上述资料的情况下，CISO 可以使用公共资源和数据泄露事件报告中披露的数据泄露事件数据进行分析。在本指南第一部分中，我们也介绍了如何利用公共资源和数据泄露事件报告来评估影响的例子。评估数据泄露影响的关键因素：1）资产价值，例如：公民、客户、员工的机密的个人身份信息、信用卡和银行账户信息 2）组织所应承当的职责。完成评估数据泄露对业务的潜在影响后，下一步是决定采取何种措施缓解风险。这是风险战略决策过程，取决于组织风险文化和组织所编列的风险优先级。

对于不同的组织类型，重中之重是做到“不要陷入非法违规”,例如一家提供在线支付处理业务的小公司因为遭到数据泄露,而导致无法符合 PCI-DSS 标准，这将导致该公司失去信用卡发行商的生意，遭受附加罚款、甚至被诉讼。对于以专利和交易信息作为关键资产的组织而言，威胁主要来自内部。

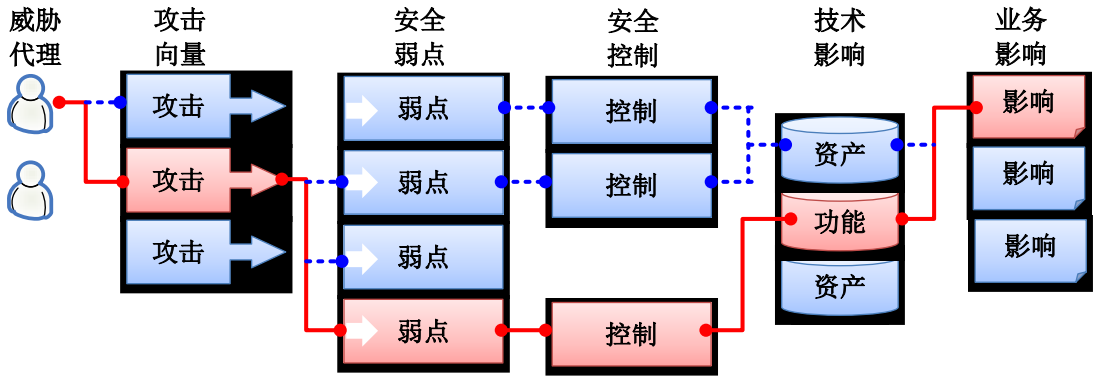
总之，应用安全应以保护数字资产为重中之重。在本指南的第一部分，我们提出了“可以用最低安全成本获得最大程度降低风险”的准则。此外，我们把安全看作是可以产生价值的而不是负担，这就是安全投资回报率（ROSI）。使用安全投资回报率来制定从战略上和战术上缓解风险的决策。从战术上，安全投资回报率用于平衡安全成本与效益，决策采取何种安全措施来缓解数据丢失所带来的风险；从战略上，安全投资回报率决策应用安全活动在软件开发生命周期中实施，从而获得长期收益。

II-3 定义风险

在展开讨论前，我们对相关术语进行定义。根据《OWASP Web 应用十大安全隐患》,漏洞的风险特征是“攻击者可通过利用应用潜在的不同途径达到破坏业务或组织的目的。每个途径代表一个可能的风险，当然这个风险可能看起来并不起眼。”

图 4 图指示攻击者可以如何采取不同的途径通过应用进行破坏

（2013 年 OWASP Top 10 WEB 应用风险）



本章主要讨论以下内容：

- 风险优先级排序
- 理解什么是“风险驱动”？
  - 威胁代理
  - 攻击、弱点（漏洞）和控制（对策）

II-4 全面风险的优先级

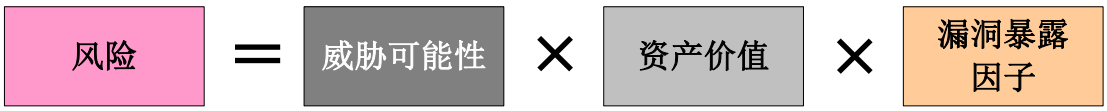
对已知漏洞的风险进行优先级排序是管控业务风险的切实有效的方法。这有助于 CISO 们确定利用漏洞或控制弱点的业务威胁的风险，也有助于明确资产与对业务负面影响之间关系。需要注意的是资产价值与资产的财务价值无关，它是相对价值。

业务风险是由系统威胁发生的概率、漏洞和资产价值组成的。

业务风险是由以下因素组成：

- 威胁发生的概率（Threat Likelihood, TL）
- 漏洞暴露概率（Vulnerability Exposure，VE）
- 资产价值（Asset Value，AV）

图 5 业务风险计算



CISO 们应该使用统一的方法用以评估已知漏洞的技术风险，例如：通用漏洞评价系统 v2.0(CVSSv2)。使用风险评估方法，重要的是将风险置于组织上下游业务链中考虑，而不仅仅是对漏洞发生的可能性和影响范围进行评估。CISO 们

通过对风险进行优先级排序进而推动应用安全防护建设。OWASP 列出了组织面临的“十大 Web 应用安全隐患”。这要求组织定期进行 web 应用漏洞的安全测试。确定漏洞及其严重程度之后，通过漏洞管理流程来管理漏洞，这有助于指导安全管理人员优先修复风险等级高且对业务影响严重的漏洞。当然,漏洞仅是缓解应用安全风险的一个方面。

关于 CVSSv2：一个风险优先级排序的方法论

在线计算 - http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2

CVSSv2 指南- http://www.first.org/cvss/cvss-guide.html

风险评价系统利用多种数据进行风险评价，包括有：

- Base Metrics
  - Access Vector (AV)
  - Access Complexity (AC)
  - Authentication (Au)
  - Confidentiality Impact (C)
  - Integrity Impact (I)
  - Availability Impact (A)
- Temporal Metrics
  - Exploitability (E)
  - Remediation Level (RL)
  - Report Confidence (RC)
- Environmental Metrics
  - Collateral Damage Potential (CDP)
  - Target Distribution (TD)
  - Security Requirements (CR, IR, AR)

II-5 理解风险驱动：威胁和对策

CISO 们通过威胁建模技术来评估风险。OWASP 应用威胁建模（https://www.owasp.org/index.php/Application_Threat_Modeling)中定义，“威胁建模是用于分析应用安全，其结构化分析方法能够识别、量化、说明与应

用相关的安全风险”。

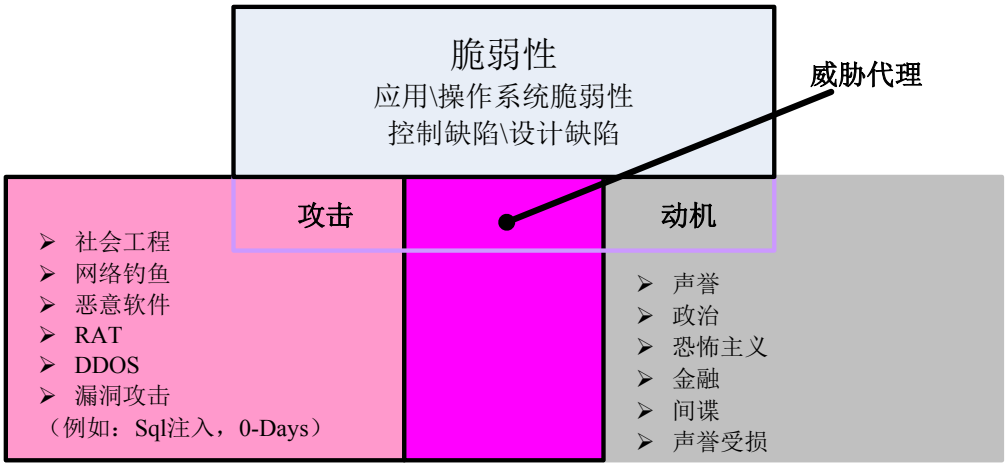
关于威胁代理

威胁代理（https://www.owasp.org/index.php/Category：Threat_Agent）：“是指实现威胁的个人或者组织。从本质上，威胁代理是识别攻击者,以及如何利用其来恶意伤害企业。”威胁代理由能力、意图和过去活动构成。

威胁代理 = 能力 + 意图 + 过去活动

威胁代理是代理动机、攻击类型和漏洞三者的交集。

图 6 威胁代理



威胁代理的日益成熟

通过识别威胁代理的意图和能力(例如：攻击类型和漏洞)，CISO 们可以评估威胁的可能性和商业冲击。随着网络威胁的发展，重要的是发现威胁代理，及其意图和过去活动(如：攻击类型)。通过分析威胁如何演变,CISO 能采取措施缓解威胁带来的风险。

在过去十年来,威胁代理发生翻天覆地的变化并日趋成熟。从历史上看,威胁代理一开始仅是机会风险。也就是说，威胁代理针对拥有相同漏洞的任何资产，而不关心该资产的价值。但如今，威胁却具有鲜明的目的性，例如众所周知的高级持续性威胁（Advanced Persistent Threat，APT)。

- 脚本小子、蠕虫和病毒作者
- 诈骗者和网络犯罪
- 黑客活动恐怖分子
- 网络间谍
- 高级持续威胁代理

脚本小子，蠕虫和病毒作者

2000 至 2005 年期间，主要威胁代理是我们称之为“脚本小子”的攻击者。他们是为了寻求出名而利用网络上找到的攻击方法、后门、恶意软件、病毒对政府系统进行恶意攻击。从历史上看，威胁代理的主要目标是计算机主机而不是网站。臭名昭著的“脚本小子”包括 90 年代后期被称为“cOmrade” 的乔纳森•詹姆斯（Jonathan James）。其拦截 3300 封电子邮件，盗取密码以及在美国国防部服务器安装后门以嗅探网络数据。2000 年，詹姆斯•约翰•阿切特（Jeanson James Ancheta）利用特洛依木马远程控制约 40，000 含有安全漏洞的计算机。同年, 由 Onel Deguzman 编写的经邮件传播的蠕虫病毒——ILOVEYOUE 蠕虫，导致全球 1000 万主机受感染，耗费 55 亿美元清除该病毒。年仅 15 岁人称“黑手党男孩”的 Michael Calce 仅用 90 分钟使用文件共享工具就迫使易趣、亚马逊和 CNN 网站下线。2004 年著名震荡波病毒(由 Sven Jascham 编写)致使约有 1000 万台主机受感染。震荡波病毒能够使卫星通讯中断、跨大西洋航班停航、金融机构和医院中断服务。CISO 们需要意识到威胁代理可以利用现成工具进行网络攻击；同时，CISO 们应当确保系统和应用无可被轻易利用的漏洞。因为一旦系统和应用存在的漏洞受攻击而导致安全事件，这不仅将可能严重影响组织运营，而且有可能经社交媒体（例如：Twitter）传播而进一步扩大对公司声誉的损害。

诈骗者和网络罪犯

2005 至 2010 年，威胁代理的动机已经从单纯地追名转变为逐利。攻击目标也从主机转向到网站，攻击动机从使用病毒蠕虫进行破坏到窃取机密和敏感数据（例如个人身份信息、信用卡和借记卡)。2007 年阿尔伯特 • 冈萨雷斯（Albert Gonzales）和其他三个同谋者分别从哈特兰支付系统（Heartland Payment

Systems)、新泽西支付卡系统、7-11 便利店、总部位于德克萨斯州的连锁便利商店、汉纳福德兄弟和一家连锁超市等成功窃得 1.3 亿张信用卡号码。黑客通过 SQL 注入攻击来获得零售商店的信用卡资料，然后他们通过篡改空白磁卡上的磁条信息从而成功地从 ATM 骗取数万美元。

2010 年，一个由 37 名俄罗斯黑客组成的网络犯罪团体利用 ZEUS 银行木马成功窃取网上银行帐户中的 300 万美元。宙斯木马是专门设计经由浏览器中间人、键盘记录器等攻击方法窃取网上银行信息的木马，同时该木马也通过会话劫持来攻击网上银行应用。

2012 年，针对银行的恶意软件正变得越来越复杂了。一款名为“游戏终结者”的恶意软件旨在窃取用户的网银登陆信息，并以此绕过多因素认证执行转帐汇款。对于金融机构的 CISO 们，了解威胁和恶意软件攻击手段从而寻求相应对策，避免因御绕过身份验证而导致安全事件。金融机构的 CISO 们也可以通过安全警示，提示客户其的个人信息、银行和信用卡信息的变更情况，从而降低因为攻击所造成的损失。

黑客活动恐怖分子

2010 至 2012 年期间出现了新一代的威胁代理，那就是出于政治目的攻击政府和企业网站的黑客恐怖分子（包括有 Lulzec 和 Anonymous）。2011 年，Lulzec 声称对索尼公司 PlayStation 网络的用户帐户和信用卡数据窃取行为负责，而同时 Anonymous 攻击 HBGary federal 网站并将其数千客户的电子邮件地址公之于众。“黑客恐怖活动分子”攻击目的是在于向公众揭露企业和政府拥有的敏感信息，而不是以经济利益为目的。需要引起 CISO 们关注的是：根据 2012 年 Verizon 数据泄露调查报告(发表于 2012 年 3 月 22 日)，尽管“黑客恐怖活动分子”所进行的攻击行为仅占 3%，但是所造成的损失却达到 58%。报告显示，大型组织是“黑客恐怖活动分子”的主要目标，他们不关心小型组织，因为对大型组织的攻击能够获得最大收益。来自著名大型企业或者公共服务组织（例如政府）的 CISO 们应该特别关注机密数据（例如：姓名、电子邮件）和机密个人身份数据（例如：姓名、身份证号）的高风险等级。CISO 们是负责政府和企业的安全，而这些网站托管和存储着其客户的机密和个人隐私信息。“黑客恐怖活动分子”出于政治

目的和需求将其作为主要攻击目标，这也正是 CISO 们所担心的。“黑客恐怖活动分子”通常利用网络钓鱼、SQL 注入、跨站脚本和 web 服务漏洞等手段攻击机构员工和客户。另一类“黑客恐怖活动分子”常用攻击手段是分布式拒绝服务攻击（DDoS）。 “黑客恐怖活动分子”出于政治考虑以 DDoS 攻击手段导致金融机构和政府机构的网站瘫痪。例如：为报复删除维基解密操作者而攻击 Mastercard.com 和 Visa.com 等信用卡网站。

网络间谍

2011 至 2012 年期间，除了“黑客恐怖活动分子”、网络诈骗和网络犯罪以外，网络间谍成为一些国际组织、政府、金融、国防和高科技工程类型的企业的 CISO 们心头之患。网络间谍热衷于窃取机密信息、金融和知识产权有关的信息。这类攻击往往利用远程访问工具（RATs）进行攻击（Shady RAT 报告,McAfee）。一份 2011 年研究报告显示网络间谍攻击行为从 2006 年中期开始至今，影响“涉及包括国防承包商、跨国企业、联合国以及国际奥林匹克委员会等至少 72 个组织”。网络间谍攻击手段有：“网络钓鱼电子邮件，通过发送钓鱼邮件给公司员工，诱使公司员工点击恶意连接，这将触发植入恶意软件”；间谍恶意软件通常与 C&C web 服务器建立后门通信信道，经嵌入网页代码解释指令编码；通过 SQL 注入传播而影响 web 服务器 (http://www.mcafee.com/uk/about/night-dragon.aspx)；以及 USB 病毒,和其他软硬件。最近研究表明网络间谍恶意软件背后或明或暗地隐藏着国家背景。

2012 年，卡巴斯基实验室确定了一款名为“高斯”的网络间谍恶意软件，它与 Flame 和 stuxnet 等网络间谍工具类似，“‘高斯’旨在窃取敏感数据，其特别关注浏览器保留密码、网上银行账户、Cookies 和受感染主机的特定配置”。

高级持续性威胁（APT）代理

网络间谍活动常与高级持续性威胁（Advanced Persistent Threats, APT）有关。高级持续性威胁（Advanced Persistent Threats, APT）的特点是采用复杂的攻击方法,比如零日攻击（zero-day 攻击）和持久性（攻击者反复攻击目标系统，且未被检测出）。谷歌、Juniper、Rackspace 和 Adobe 等都曾经遭受过 APTs

攻击。政府以及以知识产权为中心的企业也是 APT 攻击的主要目标，这都需要引起 CISO 们的强烈关注。APT 攻击还可以通过钓鱼软件，使 PC 感染木马，从而获得客户信息和雇员信息；其他 APT 攻击方法还包括攻击系统、利用漏洞以及网络间谍工具等。

关于攻击和漏洞

在本节中,我们将描述如何主动管理由特定攻击导致的风险。通常,风险缓解措施包括有修复漏洞和采用新的风险缓解对策。对应优先修复的漏洞的选择取决于对攻击场景和威胁代理的动机的理解，这包括黑客、恶意软件、导致数据资产丢失的攻击行为以及所造成关键业务损失等。风险框架是 CISO 们用于风险优先级排序的主要工具之一。应用风险取决于不同资产的内在价值和其漏洞被利用的可能性。修复漏洞之后，重要的是要评审现有安全策略的有效性,识别风险缓解措施的缺点,进而为下次可能的安全事件采取新的对策。控制差异分析可以用来决策基于安全原则选择安全策略并实施。纵深防御原则可以用来识别控制差异，并通过应用安全策略来弥补控制差异。在安全建设投资决策方面,CISOs 应该平衡成本和为缓解风险而实施的新对策的有效性。在安全建设规模上,CISO 们通过分析由于风险的可能性和影响所造成的潜在经济损失来确定安全建设投资规模。

脚本小子的攻击

对于脚本小子，CISO 需要防范他们利用脚本和通过漏洞扫描工具发现应用漏洞。脚本小子扫描网站是为了获得漏洞，发现漏洞后他们常常为了出名而将其公之于众。

对于组织而言，脚本小子对业务的影响往往是声誉上的损害，因为他们发现漏洞而不利用漏洞来破坏。对于那些由漏洞扫描工具扫描所发现的漏洞，我们认为这些漏洞是最常见的漏洞；更准确地说，这正是“OWASP 十大 web 安全隐患”所描述“广泛”和“容易检测”的漏洞，这些漏洞包括有：跨站脚本(OWASP A2 XSS)、跨站请求伪造(OWASP A5-CSRF)和错误的安全配置 (OWASP A6-Config)。对于发现 web 应用存在安全漏洞而不与漏洞的厂商联系并直接公之于众的行为，将大大增加组织的安全风险，这些漏洞可能会被用于攻击网站和窃取数据。因此 CISO

们所应做到的是密切关注脚本小子威胁和及时修补漏洞。同时，密切跟踪公共漏洞报告平台的安全漏洞信息，并与漏洞所有者及时联系，同时寻求帮助。xssed.org 网站就是一个收集和验证 XSS 漏洞的公共漏洞报告平台，它也提供对公开漏洞的修复情况进行跟踪。

CISO 们不能想当然地认为声誉损害范围限定于已被公布的既有漏洞，这些漏洞可被利用于丑化和发布未经授权的内容。通过文件注入漏洞攻击就是一个用于丑化的漏洞，例如跨框架脚本(XFS)——这是(OWASP A1:注入攻击)一部分。为缓解漏洞所带来的风险,CISO 们需要购买漏洞扫描工具用以发现漏洞，只有经漏洞扫描工具测试后的 web 应用才能发布到生产环境。此外,使用安全软件的组件和库，例如 OWASP ESAPI(企业安全 API)，有助于编程人员编写出较低安全风险的应用。

除了投资建设漏洞检测工具和使用安全软件的组件和库以外，CISO 们还可以投资建设监测和检测攻击的安全措施，例如 WAF(Web 应用防火墙)，用以防范网络攻击。这类漏洞是最容易被检测出来的，且广泛存在于 web 应用中。因此构建一套监测和检测系统用于检测脚本小子攻击行为，有助于防范脚本小子利用安全漏洞破坏系统和窃取数据。

欺诈者和网络罪犯的攻击

网络诈骗者和网络罪犯攻击网站目的就是为了获取经济利益。以信用卡支付的电子商务网站为例，电子商务网站为了完成金融交易需要获得信用卡和借记卡信息，和个人信息（包括了个人身份信息）。除了金融欺诈以外，网络诈骗者和网络罪犯的另一种攻击是获取未经授权的敏感数据，例如信用卡和借记卡数据。这些数据可用于未来的金融交易和伪造信用卡，同时个人身份信息可用于伪造身份进行欺诈。

出于经济利益的考虑，一旦有可被利用的漏洞，那么网络诈骗者和网络罪犯将不惜代价极力获得敏感数据以期控制支付与支付交易。首先，这些漏洞包括了弱认证和会话管理漏洞(OWASP A3 - 实效认证与会话管理)，即利用访问 web 应用从而获得认证数据（例如：用户名和密码），例如：伪造会话编号；跨站请求伪造(OWASP-A5-CSRF)，CSRF 可用于会话劫持从而获得非授权的金融交易数据，

包括支付和转账金额；最具破坏力的 web 应用漏洞当属 SQL 注入(OWASP - A1-注入)；其他安全风险还包括：网络诈骗者和网络罪犯可以通过传递参数而直接访问敏感数据(OWASP A4 不安全的直接对象引用)，伪造 URL 来访问这些隐藏页面 (OWSP A8-限制 URL 访问失败)，利用弱加密或者未经验证加密算法保护机密数据(OWASP A7-不安全的加密存储)和 (OWASP A9-不充足的传输层防护)。负责管理像电子商务、网上银行、保险、信贷等具有固有高风险网站的 CISO 们特别需要注重漏洞管理，及时对漏洞进行测试和修复，以防因漏洞被利用而导致业务损失。

应用层的入侵检测规则(IDS)也可以嵌入到 web 应用程序中，例如 OWASP ESAPI；或者使用 WAF(web 应用防火墙)防护网站，WAF 能够记录和监控可疑攻击行为，并触发告警。

应用威胁分析和建模可用于确定应用的风险威胁，同时也可以确定措施保护应用免受威胁的影响。从威胁分析的角度来看，在明确威胁代理、动机和攻击活动之后，需要分析可能攻击场景，确定所使用的攻击组成和漏洞。攻击树有助于理解攻击者的目标。从攻击者的角度来看，攻击者寻求经济便捷的手段开展攻击，从而获得最大的攻击成功率。如果从黑市上购买信用卡和账户数据比入侵系统更容易,更便宜,风险更低的话，网络诈骗者和网络罪犯自然就会选择从黑市上购买，而不会入侵系统。若网站拥有易被利用的漏洞，从而导致所存储的信用卡数据被窃取，那么他将成为网络诈骗者和网络罪犯的主要攻击目标。从 CISO 们的角度来看，修复应用漏洞可以减少网络诈骗者和网络罪犯利用漏洞的机会。攻击树也有助于通过网络诈骗者和网络罪犯使用的攻击模式来理解潜在威胁的实现方式。攻击树可以识别漏洞和指出最经济的防御措施。对于拥有不同的数据访问接口和信道的应用程序而言，网络诈骗者和网络罪犯最关注是最薄弱点，通过其获得最大成功概率，例如：通过攻击移动网站。安全原则之一是“你不仅仅是安全薄弱环节中的一环”, 识别薄弱点对于安全评估至关重要的。应用数据入口的识别对于确定应用的攻击面是至关重要的，其通常用于应用的威胁建模评估的一部分。

分析利用特定漏洞的威胁是另一项关键安全分析，CISO 们可以针对漏洞采取措施缓解风险。威胁树和风险框架深入分析威胁对应用和软件的影响。威胁树和风险框架实现了威胁与漏洞、威胁与对策之间的关联。OWASP 也定义了用于威胁

分析的应用威胁建模。

业务逻辑攻击

业务逻辑攻击是程序设计缺陷和逻辑漏洞，他们可被网络诈骗者利用，而且不易被测试。业务逻辑漏洞无法测试的主要原因之一是自动化漏洞扫描工具不了解具体业务逻辑，因而无法识别出。在缺乏专门人工安全测试的情况下，针对可被利用或者滥用的应用的测试，“业务逻辑攻击”漏洞是难识别和修复的，并有可能导致严重的经济损失和业务冲击。常见的利用应用的业务逻辑缺陷进行业务逻辑攻击的例子有：绕过权限访问控制从而获得未经授权的机密数据和执行未经授权的金融交易，通过攻击购物篮逻辑篡改商品价格，以及在信用卡验证签出之前篡改送货地址。业务逻辑攻击常常利用输入验证漏洞进行攻击，常见的输入验证漏洞有：交易时未对参数进行校验（例如：对角色编号、规则编号或者价格编号），缺乏对事务流程的控制，在完成交易前未对交易参数进行检查以及对权限和业务策略规则的错误配置。“业务逻辑攻击”漏洞需要通过人工测试才能被发现，人工测试是威胁建模的一部分，也是 OWASP 应用威胁建模方法论之一。

设计缺陷常常在应用安全控制设计和专门安全测试过程中被发现的。例如，密码重置逻辑缺陷，在多因素身份认证中使用可推测的挑战问题，会话无失效时间或者无法结束会话，授权和访问控制的错误配置。这些设计缺陷的常见漏洞与 OWASP A3 失效的账户和会话管理、OWASP A4 不安全的直接对象引用、OWASP A6 错误安全配置和 OWASP A8 未能限制的 URL 访问有关，并且由人工测试所识别出来。OWASP 发布了专门用于发现漏洞的应用安全测试指南。不足的反自动攻击措施（WASC21）也是业务逻辑漏洞的一种。攻击者可以使用自动化工具发布垃圾信息，也可以为了欺诈的目的使用自动化脚本枚举和验证信用卡信息（包括卡号和 PIN）。

CISO 们不能仅认为通过正常的漏洞扫描和安全测试业务就能防范业务逻辑攻击。设计和业务逻辑缺陷是需要由安全团队通过威胁建模测试对安全测试用例进行测试而发现。CISO 们应该在日常安全投资中预留用于识别和测试业务逻辑漏洞的预算，业务逻辑漏洞无法通过其它常规安全评估和测试所发现。

钓鱼攻击

网络钓鱼是网络诈骗者和网络罪犯常用的一种攻击手段,它是通过社会工程来寻找受害人,利用点击恶意链接进而下载恶意软件。网络钓鱼有针对性地选择受害人。网络钓鱼常使用包括跨站脚本(A2:XSS)，通过恶意脚本窃取 cookie 信息和运行键盘记录器等攻击方法。“OWASP A10:失效重定向和转发”主要用于让受害人访问恶意网站，从而感染恶意软件。像 XFS 漏洞这类漏洞利用网络钓鱼安装恶意软件。这些攻击都是违背受害人意愿下强制点击隐藏的恶意链接。CISO 们可以通过恶意软件查杀工具进行修复。网络钓鱼常常需要人工安全测试才能识别出来，这些安全测试包括有人工渗透测试、源代码白盒测试。对于 CISO 而言，重要的是能够招聘和培训渗透测试人员，他们与软件开发人员一样能够编写安全代码，制定安全代码评审流程、安全编码规范和使用源代码静态分析工具。

“浏览器”和“中间人”的攻击

识别和修复浏览器中间人和中间人攻击漏洞并不能保证未来就免于遭受攻击，这仅是最低水平的软件安全保障。 弹性软件要求 CISO 考虑投资安全防护对策以保护 web 应用免受浏览器中间人和中间人攻击。通过浏览器中间人攻击，网络诈骗者可以通过注入浏览器中的 HTML 字段收集加密信息、认证和信用卡数据。此外,攻击者通过键盘记录器记录受害者的认证数据。例如，在金融交易过程中，攻击者控制受害者 PC 电脑，进而劫持会话用以窃取受害者的资金。攻击人将受害人重定向到恶意网站从而耗费受害人的网络流量。

为了保护电子商务和金融 web 应用免受浏览器中间人和中间人攻击，CISO 们需要综合考虑，采取纵深防御以抵御浏览器中间人和中间人攻击，包括在客户端、在web服务器和web应用、在后端数据库和业务层等提供多层安全防护控制。在客户端，首要是让客户端免受恶意软件的威胁。通过及时打补丁、最小权限、最小安装等的简单安全防护手段就能够达到缓解恶意软件威胁的风险。需要指出的是在登录网页中嵌入安全信息提示，将有助于警示用户有关恶意软件的风险。此外，CISO 们还可以为用户采购安装查杀恶意软件的客户端软件，反恶意软件的客户端软件相对于传统的防病毒软件能够更有效地监测和查杀恶意软件。一旦客户端的 PC/浏览器感染了与网银相关的恶意软件，对于 CISO 而言，其所需考

虑的对策是增加额外的身份验证控件。同时积极的薪酬,双重验证和授权,异常和欺诈检测都是有益的方法。如果在线渠道受攻击，采用带外交易验证/支付认证和金融交易经过短信或语音的双向通知确认将使公民/客户/顾客/员工事务在安全可控状态下进行,在未经确认或者完整性校验的情况下能够终止交易继续进行。通过 WAF 和 SIEM 对带外金融交易告警数据进行告警和审计，结合诈骗行为检测分析发现异常交易率及参数,这些对于减少金融损失都将带来积极的意义(例如：暂停可疑交易账户)。

为了决策采取何种安全策略用以缓解浏览器中间人和中间人攻击的风险，CISO 们需要在成本和效益之间权衡。采用最低成本的缓解浏览器中间人和中间人攻击的风险的安全措施是 CISO 们应该最优先考虑的。通常基于客户端的反恶意软件是性价比最高的对策。针对客户的安全意识教育是最廉价的反制措施，但是客户往往会忽视安全警示。带外身份验证和带外的事务验证与授权是昂贵的解决方案，但是该解决方案有效地缓解中间人攻击，从而有效保护高风险交易。应根据实际情况决定是否采用基于监测异常流量的网络诈骗监测系统。通常，web 应用会持续遭受恶意软件的攻击,是否采用网络欺诈监测系统取决于该方法相对于其他方法是否能更有效发现网络欺诈行为。(例如：使用 SIEM 系统对交易日志进行审计)。CISO 们应有能力选择对哪些 web 应用通过修复漏洞来反制网络欺诈，哪些防御措施用以防御浏览器中间人和中间人攻击。Web 应用的风险是通过由资产价值和交易风险计算得出的。控制差异分析用于弥平识别防护和监测之间鸿沟，同时也可用于确定风险缓解的程度。采用安全防御措施后，剩余风险能够让 CISO 们明确是接受风险，还是需要进一步采用额外的控制。

拒绝服务攻击（DoS）

拒绝服务攻击（DoS）会严重影响网站的可用性，可能会导致组织收入的损失。CISO 们应当把防范拒绝服务攻击作为其工作的重中之重，尤其是线上业务是赢利来源的 web 应用，以及将可用性作为重要指标的应用。

拒绝服务攻击往往利用 web 应用的漏洞,DoS 曾经在 2004 版 OWASP 十大安全隐患中上榜（OWASP A9:DoS)，但由于 2006 年 MITRE 排名而于 2007 年从 OWASP 十大安全隐患中删除。虽然,DoS 不再是 2010 版 OWASP 十大安全隐患中的一员，

根据风险和资产价值的影响，可导致拒绝服务攻击的漏洞应该是高风险漏洞，并应该被优先修复。在应用级别,拒绝服务攻击会利用注入攻击，特别是可能会因为 SQL 注入、XPATH 注入、LDAP 注入而导致应用崩溃。在用户层面，拒绝服务攻击可以导致注册用户应用的瘫痪。我们可以通过以下攻击场景理解这个过程：攻击者通过脚本对所猜测出的用户进行锁定，或者通过异常登陆导致用户账户锁定。在无自动账户解锁的策略下（例如：24 小时内将自动解锁已被锁定的用户帐户），用户无法正常登录，这将导致大量客户致电呼叫中心寻求对账户解锁。在代码级别，DoS 利用不安全的代码耗尽计算机资源。例如，内存泄露导致程序异常崩溃。其他的不安全代码案例还包括：空指针和恰当的中断、无法捕获的异常和利用 XML 解析引擎对恶意递归 XML 文件解析导致内存耗尽。针对像 C 或 C++语言而言，错误的内存分配和使用不安全函数都有可能导致源代码的暴露和缓冲区溢出攻击，从而导致应用程序崩溃或被控制。缓冲区溢出漏洞是服务器级别，对于那些不及时打补丁的 web 服务器和 web 应用易受缓冲区溢出攻击。CISO 们应确保在应用和代码上线前进行安全测评，通过安全测评工具（包括有静态和动态应用安全测试工具）及时发现可被利用的拒绝服务攻击漏洞。

分布式拒绝服务攻击（DDoS）

在传输层和网络层层面，拒绝服务攻击通常利用网络层协议类型的漏洞（例如：伪造包）制造出网络流量泛洪攻击。分布式拒绝服务攻击通常使用僵尸网络对网站发起大流量泛洪攻击，大流量的网络请求超过了 web 服务器所提供的能力，因而无法应答来自网络的请求并拒绝为用户提供服务。通过以下措施有助于缓解拒绝服务攻击的危害：通过托管的数据中心对异常流量进行过滤和采取其他防御措施；采用纵深防御手段可以为组织防御 DDoS 攻击提供早期预警和尽早采取过滤异常流量的措施。纵深防御措施尽管能够缓解攻击者的攻击，但是它还不足以阻断 DDoS 攻击，还需要结合其他安全防御措施。根据木桶原理，采用简单和开放的安全机制可以安全地实现管理和审查，以最低权限为原则实施安全访问控制。

下面介绍一下常见的 DDoS 攻击，例如“Ping of Death”僵尸网络通过伪造海量包导致目标服务器瘫痪，“邮件炸弹”僵尸网络发送海量邮件导致邮件服务器瘫痪，“Smurf 攻击”通过发送 ICMP 包反射放大拒绝服务攻击攻击，“Teardrop”

僵尸网络通过发送畸形包导致目标服务器瘫痪。

如今，“脚本小子”、黑客恐怖活动分子、网络罪犯和由国家资助的黑客通常利用开源 DDoS 工具和僵尸网络来制造 DDoS 攻击。公共和私人组织是常见的 DDoS 攻击目标。通常这些 DDoS 攻击是为了出名和损害公司声誉。DDoS 攻击的动机取决于威胁代理的类型和动机。“脚本小子”通过 DDoS 攻击希望能够找到可以利用的 DDoS 漏洞从而获得恶名；“黑客恐怖活动分子”出于政治目的用 DDoS 攻击从而获得媒体的关注；网络诈骗者和网络罪犯为了骗取网上银行客户而实施 DDoS 攻击；由国家资助的黑客则出于经济和军事的目的对他国网站进行攻击破坏。DDoS 攻击所产生的损失取决于受攻击的网站类型、攻击时长和受影响的用户数量。DDoS 攻击所导致的业务损失可以由因网站下线受损失的业务来计算得出。根据“第二届网络犯罪研究的年度成本基准研究”（2011 年 波耐蒙研究所），该研究涉及 50 个组织和美国公司，DDoS 所造成的损失达年均$187,506 美元。这个计算结果是依据对所有受调查公司的 DDoS 攻击事件概率的加权平均。另一项由 CA 公司主导，涉及 2 0 0 家在北美和欧洲公司受 DDoS 攻击影响的调查研究表明因为 DDoS 攻击导致服务器下线所造成的损失年均达$150，000 美元。这些估算结果是根据 DDoS 攻击针对不同的在线业务和受影响的范围估算出来的。对于大型电子商务网站，以亚马逊为例，其 2011 年收入达 480 亿美元。一旦因为 DDoS 攻击导致在线业务中断，每小时损失达数百万美元。对于像电子商务网站和金融网站等在线业务是其公司主要收入来源的 CISO 们而言，缓解 DDoS 攻击是其工作的重中之重，应优先考虑采取抗 DDoS 的防御措施以缓解 DDoS 攻击所带来的风险。如今 DDoS 攻击非常普遍，这主要是因为攻击者可以以非常低廉的成本租用 DDoS 攻击的工具和僵尸网络执行 DDoS 攻击。根据“DDoS 攻击经济因素的模型：Femtocell 案例研究”（来自哈维尔·比森特和塞古拉·Lahuer，西班牙电信网络与安全服务部），租用 DDoS 攻击的僵尸网络的成本约 100 美元每天 1 Gbps 的带宽。

CISO 们必须意识到 DDoS 攻击的严重性和复杂程度也日益增加。根据 2011 年“第六届全球基础设施安全报告”(来自：Arbor Networks)，过去六年间，DDoS 攻击危害增加了 10 倍，达到 100Gbps。DDoS 攻击能力的提升不能仅归因于 DDoS 攻击工具的复杂程度，新的 DDoS 攻击手段进一步放大了攻击效果。分布式反射

器拒绝服务攻击(DRDoS)就是新一类的 DDoS 攻击方法。它利用向 DNS 服务器发送伪造的受害者的源 IP 的 DNS 解析请求，这样就以僵尸网络向 DNS 服务器发起 DNS 解析请求从而放大了攻击。

传统网络层的抗 DDoS 攻击措施有：黑洞路由、地址过滤、限速和网络过滤。但是上述方法不足以抵抗 100Gbps 以上的 DDoS 和 DRDoS 攻击。为了抗衡大流量的 DDoS 和 DRDoS 攻击，CISO 们为保障网站可用性可以采用以下措施：划分网段、通过 CDN 服务提供静态内容和使用第三方基于云技术的 DDoS 防护服务(参考 Attacks FS-ISAC_Threat_Viewpoint_DDoS_June_2012.pdf)。

II-6 的缓解新应用技术的内在风险

编写本章节的目的是指导 CISO 应对在采用新技术（包括有移动技术、web2.0 技术和 SaaS 等)之后而引入的新的安全风险。随着技术的发展，对于 CISO 而言，重要的是了解引入新技术所带来的安全风险，新技术的引入为攻击者提供新机会用以攻击应用和数据。采用新技术(例如将应用扩展到移动设备上、采用 WEB2.0 技术、使用云计算等)将导致攻击面的扩大。为了缓解因采用“新技术”而引入的新安全风险，CISO 需要清晰认识所面临的安全风险，决策所采用的新应用安全评估手段、工具和安全措施。

管理移动应用的风险

面对移动智能手机和平板电脑在个人和商业领域爆炸性的增长，对于大多数组织来说应该特别关注“移动应用安全”。从应用安全角度来看，通过移动设备访问商业应用增加了威胁代理对移动终端、应用和数据的威胁机会。以手机安装恶意软件为例，不仅手机终端可被安装了恶意软件，同时应用可以获得手机终端信息。通过不同移动信道（包括有 WIFI 网络、MMS、短消息、2G、3G 和 4G 网络）可以攻击包括 web 在内的不同业务。采用移动终端访问应用的企业应该认识到采用移动应用必然遭受攻击的可能性。因此，要求对移动应用的安全性和存储于移动终端的敏感数据的防护进行专门的漏洞评估是重要的。要求对存储于移动设备上的机密和认证数据进行加密，这样操作可以满足内部移动安全标准和策略的合

规要求。对于允许移动终端访问的 web 应用也需要进行安全评估。一般情况下，组织应避免在移动终端进行具有固有高风险的金融交易（例如转账和支付），因为移动终端的认证措施相较于基于 PC 的互联网应用而言还不足够安全。在某些情况下，设备安全控制同样也是不够安全，例如：使用基于设备的加密（iOS 秘钥链），因为用户丢失移动终端后可能遭受到暴力破解。这些重要的风险因素存在，就必然要求开发团队在开发移动应用过程中严格遵循安全标准。

除了移动终端存在丢失或被盗的风险以外，移动终端可被安装键盘记录器也是另一类安全风险。移动终端被键盘记录器之后，其可以记录用户的认证信息并将数据上传至服务器。如今，移动应用为通过像电子邮件、社交媒体、视音频流媒体、即时通讯和网页等的不同通信信道攻击手机中的应用提供了可能。例如：移动终端用户点击邮件中的恶意链接下载并安装移动间谍软件和远程访问工具。移动恶意软件形势严峻，有一类专门用于攻击网上银行身份验证的时间令牌的移动恶意软件，他们能够利用移动中间人攻击（MiTMO），获得受害者移动电话的一次性认证口令，然后由该恶意软件转发一次性认证口令、用户名和密码给网上银行。另一种移动应用攻击渠道是移动应用商店（例如：应用商城和 Apple Store），Android 和 iOS 应用占全球智能手机应用的近 90%，因此通过应用商城来传播恶意软件是最好的途径。一些移动应用商城有专门针对应用的安全检查，例如 Apple Store，这有效缓解了下载恶意移动应用的风险。但并不是所有的应用商城都对移动应用进行安全检查，因此应将其视作安全风险。

只要移动用户采取基本安全防范措施，就能够获得足够的安全。在某些情况下，缺乏基本简单的安全措施，例如未使用 PIN、通过“越狱”安装应用，都将增加该移动终端上的数据和应用的安全风险。通过给移动设备用户持续性安全警示和推荐采用简单实用的安全防范措施都是良好的安全防范措施。针对手机的安全意识和防护手段可以参考《移动手机的网络威胁》（美国 CERT）

对于负责管理移动应用安全的 CISO 们来说，重要的是考虑采取什么专门安全措施和标准以满足移动应用安全需求。CISO 可以采取的安全防护措施有：采用和记录移动安全标准、针对移动应用的漏洞执行漏洞评估，以及针对存储于个人消费终端的应用与数据的安全配置的标准。在为移动应用漏洞进行专门安全测试流程方面上，OWASP 移动安全项目拥有很多资源，例如：移动设备上的文档安

全风险，免费漏洞评估工具、检查清档和移动应用的安全设计指南。

在移动安全领域，确保由组织签发的移动终端以及由个人带进机构的移动终端（如：BYOD）的安全是 CISO 们需要引起关注的方面。随着移动终端的普及，移动终端在企业内使用正越来越普遍。CISO 们需要评估潜在安全风险，并明确如何授权存在潜在安全隐患的员工移动终端。如今，一些组织可能允许员工使用其移动终端通过安全连接工具（包括有 VPN、安全虚拟化、终端服务器或者其他远程访问工具（例如：VNC））访问组织内部网络。CISO 要制定远程访问策略以管理员工通过其移动终端远程访问移动应用，从而确保移动终端能够安全地、集中化地、受控地使用远程访问技术和服务。以下标准规范指导 CISO 管理 BYOD 和集中化管理安全移动设备，包括有 NIST SP 800-124，《管理与保障企业移动设备安全指南（草案）》和《手机与 PDA 安全指南》。

管理的 Web 2.0 技术的风险

新技术的引入，必将带来新的安全风险，同时与之对应的防御措施也应到位。针对新技术可能带来的影响，CISO 提前计划采用相关安全措施和流程来缓解风险。Gartner 采用技术成熟度曲线分析评估新技术，包括五个阶段：

(1)上升期

(2)快速发展期

(3)下降期

(4)爬坡期

(5)稳定应用期

在 2009 年发布的技术成熟度曲线分析中，Web2.0 在未来两年内将得到广泛应用。这个预测得到了市场的验证，目前一些 web 应用采用和集成了 web2.0 技术。Gartner 和 Forrester 的研究报告有助于 CISO 洞察技术趋势和安全风险趋势。首先，我们定义“什么是 web2.0 技术？”。Web2.0 技术就是“促进互动信息共享和协作、良好互操作性、以用户为中心的 web 应用”。Web2.0 主要技术特点有：

- 鼓励用户通过社交网络/网站参加虚拟社区，并互相协作。用户可以自己添加更新内容，例如 Twitter、Facebook、Myspace、LinkedIn、YouTube

等。

- 使用新技术/框架。包括有 AJAX、Adobe AIR、Flash、Flex、Dojo、Google Gears 和其他。
- 组合和聚合来自不同应用和系统的数据,例如：通过“mashup”将不同客户端功能聚合(例如 web 服务,SaaS)。

CISO 们应注意 web2.0 技术所带来的安全风险。首先，web1.0 所面临的安全风险,必将在web2.0技术上进一步放大,因为web2.0用户之间的交互更加频繁：考虑到拥有数百万用户的社交网络和 web 应用所增加的攻击面,威胁代理通过网络钓鱼手段利用恶意链接攻击 Facebook 和 Twitter 用户,这与传统 web1.0 漏洞（注入攻击、XSS 和 CSRF）攻击行为类似。用户可以通过社交网络分享机密和私人信息,但这存在用户在未经公司许可下分享了未经授权的公司机密信息的安全隐患。

对于 web2.0 而言，不同 web2.0 技术和服务的集成导致功能的复杂性增加，这也是 web2.0 技术增加的安全风险的因素之一。富客户端增加了业务逻辑遭受攻击的可能性。

可被攻击者利用的 Web 2.0 安全漏洞

由 web2.0 技术引入的风险，对于 CISO 们而言，重要的是确保 web 应用通过采用专门设计、实现和测试以缓解新增加的风险。从漏洞和威胁分析角度看，web2.0 漏洞可以通过 OWASP 十大安全隐患和 WASC 前 50 大安全威胁进行安全风险分析。Web2.0 应用需要测试包括 A1-注入，A2-XSS，A3-失效认证与会话管理和 A5-CSRF。下面我们介绍 web2.0 的一些注入攻击手段：XML 注入漏洞——攻击者提供未经校验的输入插入到 XML 中，从而影响 XML 文件的结构和标签(而不仅仅是内容)。XPATH 注入是一种特殊的 XML 注入攻击。XPATH 注入攻击旨在篡改 XML 查询从而获得敏感数据。JSON 注入是另一种 web2.0 专门的注入漏洞，其通过运行未经授权的代码，利用客户端将恶意 Javascript 脚本注入到 JSON(JavaScript 对象表示法结构)

RSS feed 注入攻击能够让用户订阅不受信任的 RSS feed 资源，从而下载恶意软件进而在受害者计算机执行。Web2.0 的 XSS 攻击手段是利用 web2.0 网站允

许用户在内容中添加 HTML 代码，例如用户发布博客、留言板等。如果 HTML 数据未经过滤，攻击者在 HTML 标签中注入恶意代码用于 XSS 攻击。另外一种 Web2.0 XSS 攻击载体是 XSS DOM，富客户端应用常使用 DOM，例如 FLASH、Sliverlight。AJAX 的使用也增加了 XSS 攻击的可能。Web2.0 注入漏洞攻击事件案例：WHID 2008-32，Yahoo HotJobs XSS 漏洞可被威胁代理利用窃取会话 Cookie 信息。

在 Web2.0 应用中，攻击者可利用的 OWASP-A3：失效认证与会话管理漏洞，包括有弱密码、密码存储于 AJAX 小部件/Mashup 并明文传输、密码存储于客户端并使用“自动登录”功能，以及在云平台使用单点登录和密码恢复机制（因为不锁定尝试登陆攻击，无法防范暴力破解）。参见 WHID 2008-47: 联邦供应商指南在 Javascript 中验证登录信息。

CSRF 也是 web2.0 常见的漏洞之一。通过以下案例来了解，CSRF 针对 web2.0 应用得攻击。当客户使用 AJAX 通过 XHR 调用 web 应用时无法直观验证其伪造。利用浏览器针对桌面部件缺乏足够的单一来源策略管控进行 CSRF 攻击，利用设置超长会话失效时间导致的弱会话管理进行 CSRF 攻击。通过小部件共享的持久会话 cookie 同样会增加 CSRF 攻击的机会。与 CSRF 有关的 web2.0 安全事件案例有：WHID2009-4“Twitter 个人信息 CSRF”——攻击者利用 Twitter 的 CSRF bug 获得访问者的个人信息。

缺乏抗自动化防御的漏洞也是可被利用攻击 web2.0 应用的漏洞。虽然其不是 OWASP 十大安全隐患之一，但却是 WASC50 大安全威胁之一，位列第 21 位。针对 web2.0 应用，通过自动化攻击滥发垃圾留言、博客和微博信息，并通过这些恶意网站传播恶意软件。

Example: Insufficient Anti-automation for Facebook In 2007, Facebook was accessed through automation in an attempt to harvest user information.See WHID 2007-65:” Botnet to manipulate Facebook”

缓解风险的安全措施

分析 web2.0 漏洞的关键是确定漏洞的根本原因。只有识别漏洞产生的根本原因，漏洞才能根除。对于那些来自缺乏安全需求的 web2.0 应用的漏洞而言，他们需要用文档记录下来，在设计过程中这些问题触发错误，为防止漏洞产生，

需要有 web2.0 经验的安全架构师对所设计的 web2.0 应用进行审查。为防止因为软件开发人员的编码错误或者集成第三方软件或第三方类库而带来的 web2.0 漏洞，重要的是对应用软件开发人员进行编码规范性培训、安全测试人员要知道如何识别和测试 web2.0 漏洞

以下 web2.0 安全措施有助于 CISO 们规避风险：

- 使用文档记录与 web2.0 技术相关的安全标准，例如设计、编码和测试专门 web2.0 技术的安全需求，包括 AJAX、FLASH；在软件开发周期中严格执行。
- 研究 web2.0 应用潜在威胁，并确定应用威胁模型等对策。还需要对应用架构和安全控制措施的安全审查。安全控制措施包括了针对输入验证、身份验证、会话管理和反自动攻击的控制措施，如：验证码。
- 要求基于 web2.0 应用接受安全代码审查，以确保源代码符合安全编码规范；通过静态代码分析来识别 Web 2.0 客户端编码问题源，包括代码所使用的小部件,RIA,AJAX 组件以及服务器端代码中所使用 Web 服务和 SOA。特定的安全代码需求可以经 AJAX 记录，这些可以在涉及和代码审查阶段由架构师和软件开发人员进行评审。
- 安全测试包括针对 web2.0 组件漏洞的测试用例和针对 web 服务的测试用例。可以参考由 OWASP 制定的测试 AJAX 和 web 服务的测试指南。

确保 web2.0 技术风险是可管理的，web2.0 技术风险包括有例如由 web2.0 应用的设计缺陷和 bug 引入的业务风险。OWASP 风险方法论可用于管理 web2.0 安全风险。以下定义了 web2.0 技术的 OWASP 风险框架。

表 1 适用于 Web 2.0 技术的 OWASP 风险框架

威胁代理	滥用和 攻击向量	安全弱点	安全控制 /对策	技术影响	业务影响
Web 2.0 的用户	用户共享的私有/保密信息，代理发布机密信息	控制用户固有的缺陷导致的社交网络内容，博客，即时消息，私人电子邮件	Web 2.0 的社交网络的安全策略，合规性监控，过滤，归档，社交网站帖子的审批工作流	敏感/机密数据较少	声誉受损，合规失效罚款
恶意用户，诈	受害者目标	社会工程学，	用户教育，数	在客户端执	欺诈，财务损

骗者	是通过网络钓鱼，恶意小工具下载，点击恶意的帖子	Web 2.0 的漏洞：XSS	据过滤，转义/编码不可信数据	行 JavaScript，安装恶意软件	失，篡改，声誉受损
恶意用户，诈骗者	攻击者通过发送恶意数据到应用程序的接口	Web 2.0 的漏洞：XPath 注入，XML 注入，JSON 注入	筛选，参数化的 API，ESAPI 过滤方法，白名单验证	数据丢失，数据篡改，拒绝服务/访问	公开披露，声誉受损
恶意用户，诈骗者	攻击者利用认证或会话管理功能的漏洞或缺陷	Web 2.0 打破身份验证和会话管理漏洞	实现安全密码策略，帐户锁定，禁用自动登录的安全要求	未经授权存取数据，功能	C. I. A 损失，法律和财务问题
诈骗者	攻击者创建伪造的 HTTP 请求欺骗受害者提交请求的技巧	Web 2.0 的跨站请求伪造漏洞	包括在一个隐藏字段中的唯一令牌	可以更改数据，并代表用户的开展功能	C. I. A 损失，欺诈，拒绝访问
自动化脚本/垃圾邮件机器人	应用请求链接，创建账号，游戏应用，擦除数据	抗自动化能力不够	行为监控，应用传感器攻击检测，包括验证码，ESAPI 入侵的 API	可以溢出程序的垃圾邮件，枚举	业务中断/损失，声誉受损

管理云计算服务的风险

云计算并不是一个崭新的名词。过去,许多组织将其数据中心外包给第三方所有的数据中心，这可以认为是 IaaS 云服务的雏形。云计算包括有基础设施即服务(IaaS),平台即服务(PaaS)和软件即服务(SaaS)。

CISO 如今所面临的挑战在于评估和确定私有云或公有云的安全性。对于组织而言，将基础设施、平台或软件和数据托管于第三方的云服务提供商，CISO 最顾虑托管于第三方运服务提供商的信息和应用的安全。CISO 们需要评估潜在风险之后才能决定是否把服务外包给第三方云计算提供商。CISO 们之所以顾虑管于第三方云计算平台的数据的安全性,是因为安全事件常常发生在云计算服务提供商。CISO 们还必须了解到第三方云服务提供商所提供的数据服务可能因为遭

受到拒绝服务攻击导致其提供的服务不可用,进而影响到组织的业务。

因此,CISO 应做到在组织决策将服务或数据迁移到云平台之前评估所面临的信息安全风险。CISO 可以通过第三方信息安全评估机构对云计算服务供应商进行尽职调查。安全评估需要涵盖云计算服务提供商所提供的安全活动是否符合公司信息安全策略、相关行业标准与规范（包括有 SAS70、SOC、FISMA、PCI DSS、ISO、FIPS-140、ISO/IEC 27001-2005 等）以及合规准则（包括有 HIPPA、FFIEC、MPAA 等）。

云计算安全评估需要覆盖安全风险、合规审计与云架构、治理、法律法规、隐私保护、业务连续性和灾难恢复、应急响应、应用安全、加密和密钥管理、身份管理、权利和访问管理、虚拟化和安全即服务等领域。

云安全联盟(Cloud Security Alliance, CSA)的职责是指导如何监管云计算所涉及各项安全领域。CSA 拥有一系列的安全评估工具用于评估云计算安全风险，涉及领域包括有 SaaS,PaaS 和 IaaS 信息安全、合法合规、组织策略、风险管理、弹性和安全架构,和对标准的合规（例如 COBIT4.1,ISO 27001,NIST SP 800 - 53，PCI-DSS vs 2.0 等）。CSA 评估计划调查问卷 v1.1 可以让 CISO 们对第三方云计算服务提供者所提供的信息安全合规、数据治理、设备安全、人力资源安全、法律、业务管理、风险管理、发布管理、弹性和安全架构进行评价。2013 年 CSA 还发表了一份用于指导缓解云计算前九大安全威胁的白皮书

云计算九大安全威胁

（https://cloudsecurityalliance.org/）

1. 数据泄露
2. 数据丢失
3. 账户劫持
4. 不安全的 API
5. 拒绝服务攻击
6. 恶意内部管理人员
7. 云服务滥用
8. 未尽职
9. 共享技术

OWASP 建议 CISO 们可以使用 CSA 指导文档、调查问卷和威胁分析指南用于构建专门的云计算安全评估流程，并由组织的信息安全团队执行云计算安全评估，并对云计算提供商所提供的信息安全、风险和合规审计进行尽职调查。专门的云计算安全评估流程应基于组织的信息安全政策、相关标准和法规，从而确定云计算提供商的安全性，保障数据的机密性、完整性和可用性。专门的云计算安全评估过程通过一组调查问卷用于捕获和发现云计算安全提供商的安全、合规和风险管理现状，做出是否外包服务（基础设施、网络、平台和软件及数据）的结论。云计算安全服务评估的主要目的是确定控制差异和潜在的风险领域。云计算安全服务评估可以识别以下可能的应用安全风险，包括有缺少端到端的加密，业务数据传输过程和存储于第三方云计算提供商的机密性，缺少在虚拟化环境下与其他企业的数据隔离，缺少对安全事件的日志审计。为缓解风险的安全控制，可能采取以下措施用以缓解应用安全风险：使用端到端的加密，使用虚拟防火墙和采用安全 hypervisor 架构来保护租户在 SaaS 云虚拟环境下的安全，采用专门的日志审计手段。

控制差异识别之后，接下来要做的是对风险进行定级和确定采取的安全措施。此外通过服务水平协议（SLA）来捕获风险也是重要的一个方面，要求在云服务提供商所提供的合同协议条款和赔偿责任中明确对 SLA 要求，以防对 SLA 的违约。

（本部分翻译 陈冬冬）

第三部分：应用安全计划

III-1 内容提要

从整个风险管理策略来看，应用安全风险的缓解不是一次性的活动，而是一项持续的工作，需要密切关注新出现的威胁，并部署和规划新安全措施，以消减这些威胁。

包括规划新的应用安全活动、流程、控制措施和培训。规划新的应用安全流程和控制措施对于 CISO 而言非常重要，他们知道在哪些应用安全领域进行投资，可以使企业实现其使命。

要建立和发展一个有效的应用安全计划，CISO 们必须：

- 映射业务优先级到安全优先
- 使用安全计划的能力成熟度模型评估当前状态
- 使用安全计划的能力成熟度模型建立目标状态

映射业务优先到安全优先

所有的安全优先级必须能够映射到业务重点。这是旨在建立每一个安全起步并表明企业管理安全如何支持使命第一步的重要性。它还演示了保安人员如何支持工作人员的使命。

使用安全计划的成熟度模型评估目前的状态

访问过程的成熟度是通过应用安全和软件安全过程的先决条件。常被组织采纳的标准之一就是要考虑组织在应用安全领域的能力和组织的在这些领域操作的成熟度。这些应用安全领域的例子包括应用安全治理、漏洞风险管理、合规性和应用安全工程，如设计和实现安全的应用。特别是在应用安全工程的情况下，采用软件安全保障往往是必要的，而没有实施这类软件安全性，是因为它由第三方供应商直接控制生产的。在这种情况下要考虑的一个因素是使用成熟度模型来衡量软件的安全保证。采用安全的软件开发生命周期（ S- SDLC ）测量软件的安全保证是一个先决条件。在高级 S- SDLC 包含软件开发生命周期内的培训和工具

中“构建安全”的安全活动 。这些活动的例子可能包括软件的安全流程/工具如构建风险分析/威胁建模，代码的安全性评价/静态源代码分析，应用安全测试/应用漏洞扫描和软件开发人员安全编码。OWASP 软件保证成熟度模型，以及几个专用于软件安全的 OWASP 项目和 S-SDLC 和本指南都可以做为参考。

使用安全计划的成熟度模型建立目标状态

并非所有的组织都需要达到最高的成熟度。成熟度应该维持在一个能够管理影响业务安全风险的水平。显然，这在不同的组织之间有所不同（变化），并且这和业务有关，以及能接受的作为来自安全组织的持续合作以及透明度的一部分的风险有关。

一旦目标状态是确定的，CISO 应该建立一个确定其解决已知问题的战略，以及检测和减轻新风险的路线图。

OWASP 提供了几个项目和指南，来帮助首席安全官制定和实施应用安全计划。除了阅读本节中德指南，请参阅附录 B：OWASP 指南和项目高效参考，可以获得能够纳入应用安全计划的安全工程领域的活动类型的详细信息。

III-2 简介

缓解寻求利用保护和检测控制应用漏洞导致的攻击风险以及潜在的差距是 CISO 主要关注的问题之一。如果漏洞是在安全事件发生后才被发现，下一步是修复漏洞并限制进一步的影响。通常情况下，这涉及漏洞修补实施后重现和重新测试漏洞，以确保漏洞不能再被利用。如果该事件是由于安全控制措施的缺陷诸如未严格过滤恶意的输入或检测到攻击事件，下一个步骤是采取对策来降低风险。对策可能是威慑，预防，检测，纠正，补偿等安全控制措施的组合。CISO 需要考虑漏洞以及安全控制措施的弱点的风险，就如何降低风险作相应的决定。通常修复一个漏洞涉及到漏洞管理周期，其包括识别漏洞，修复漏洞，然后重新测试以确定它不再存在。

在应对措施被部署之后，对于应对措施可以用一个功能的安全性测试对其有效预防和检测到攻击向量进行测试。决定部署哪些应对措施可能会取决于不同的

因素，如应对措施花费的成本与安全事件对业务的影响，以及应对措施对风险的有效缓解的程度的比较。对于 CISO 而言，在这之后下一步要做的是使安全事件得到控制，确保任何弱点得到修复，应对措施得以部署以消减风险。在指南的本小节，我们专注于第 2 部分中确定问题的最具成本效益应用安全措施目标。例如如何划分整个软件安全活动，如安全代码的培训，安全代码审查，安全验证和测试问题和风险管理。

在 2013 年的 CISO 调查中，CISO 确定他们的首要任务和他们的计划所面临的风险。在本指南中，你会发现不仅对执行这些首要任务的工具和流程的指导，而且指引管理可能会影响你的首要任务的风险。

2013 CISO 调查：CISO Top 5 优先级任务
1．安全意识和开发培训
2．安全开发生命周期流程（例如，安全编码，QA 流程）
3．应用安全测试（动态分析，运行时观察）
4．应用层的漏洞管理技术和流程
5．代码审查（静态分析源代码，找出安全缺陷）

在同一个 2013 CISO 调查中这些优先级是由 CISO 们确定的抑制高风险任务，如下所示

2013 CISO 调查：CISO Top 5 风险
1．组织内部缺乏应用安全问题意识
2．不安全的源代码开发
3．缺乏的/不足的测试方法
4．缺乏预算以支持应用安全举措
5．人员配备（例如，团队内缺乏安全技能）

III-3 应对 CISO 的应用程序的安全功能

应用安全治理，风险和合规性

治理是引入了政策、标准、过程和策略集合、目标和组织结构以支持它们的过程。在操作层面，治理、合规性和风险管理是相互关联的。作为治理职责的一

部分，CISO 影响应用程序的安全目标，并与高级管理层合作去设置应用安全的标准，流程和组织结构，以支持这些目标。作为合规职责的一部分，CISO 与审计师及法律顾问合作，以获得信息安全政策，建立需要遵守的需求，测量和监控这些需求包括应用安全需求。作为风险管理职责的一部分，CISO 识别，量化并进行风险评估，以确定如何消减包括引入新的应用安全标准和流程（治理），新的应用安全需求（合规性）和新的应用安全措施（风险和控制）而带来的应用安全隐患。从治理的角度看，在任何特定组织内，采用的应用和软件安全流程，应用安全团队和应用安全标准的建立依赖于组织的行业类型，组织的规模和 CISO 在该组织内扮演的角色和承担责任。 OWASP 为 CISO 提供了几个项目和指南，以帮助他们制定、实施和管理应用安全治理。请参阅附录 B ： OWASP 项目和指南在治理领域快速参考的详细信息。通常，应用程序安全投资的来源也根据组织规模和组织的类型各不相同。因为 CISO 向组织的信息安全运营和风险管理的首脑报告，一般用于应用程序安全的预算是分配给信息安全和操作风险部门的整体预算的一部分。对于这些 CISO，采用新的应用安全活动如 OWASP 提供的那些指南和工具的一个主要原因，首先是要满足合规性和降低组织资产如应用程序和软件面临的风险。合规性的多样性很大程度上依赖组织所在的行业和该组织所服务的客户类型。例如，软件生产厂商生产政府如美国联邦政府部门和机构使用的加密软件，需要遵守联邦信息处理标准（FIPS ）140。软件生产厂商生产处理持卡人数据，如信用卡和借记卡支付数据，需要遵守支付卡行业数据安全标准（PCI DSS ）。向组织的信息技术首脑报告的 CISO，通常负有安全和信息技术两方面的职责，可能还包括应用和软件技术与安全标准的合规性，如 FIPS 140 和 PCI -DSS。符合安全技术标准，代表了在组织内促进安全开发和测试的机会，如使用 OWASP 安全测试指南，获取应用程序和软件产品安全认证。符合 PCI -DSS 要求，例如，可能要求组织已经测试应用程序常见的漏洞的最小集合，如 OWASP Top 10。IT 部门为获取技术安全标准认证分配的预算，如 FIPS -140 和 PCI -DSS，也可用于推广安全编码指南，如 OWASP 的安全编码指南，或者投资于静态代码分析工具。例如，在符合 PCI -DSS 的情况下，CISO 可能会选择静态代码分析，以满足 PCI-DSS 标准的要求 6.6 。 OWASP 为 CISO 提供了几个项目和指南，以帮助制定和实施策略，标准和应用安全指南，并帮助定义进行验证和审核的应用安全需求。请参

阅附录 B ： OWASP 项目和指南在标准和策略、审计和合规性领域快速参考的详细信息。

小企业的 CISO 也可以使用漏洞管理方法来实现这样的业务，在 SDLC 的不同阶段投资安全，改善软件的质量和安全性。例如，大部分的质量问题和安全问题是因为编码错误导致的，强调 IT 部门需要采取安全编码流程、标准和对开发人员进行培训对 CISO 来说非常重要，因为专注于这些软件安全活动可以节约组织的成本。从 NIST 的一项有关解决安全问题花费成本的研究表明，在软件发布之后修复代码问题的成本比在编码时将其修复花费的成本高 6 倍多。为了实现节约金钱和提高效率的目标，CISO 可以与工程部经理一起工作，以促进应用和安全软件的举措得以实施。CISO 指南的第四部分提供了有关用于管理应用安全风险的指标，和对应用安全的投资的决策的指导。

在 CISO 的职责当中，业务的连续性（COB）对于向客户提供关键业务功能的 Web 应用来说是最重要的。CISO 负责推出的 CoB 计划，以确保即使不利的情况或事件发生，业务也能继续运行。一个 CoB 计划包括恢复因为一个负面事件而失效的服务，例如一个托管 Web 应用的数据中心断电时。 CoB 计划的一个重要项目是识别被视为关键业务的 Web 应用，并指派重要性和 CoB 测试的具体需求，如服务恢复的最长时间要求。和 CoB 一样，灾难恢复计划也是 CISO 的职责之一：这包括因为自然或者人为的灾难后恢复或延续技术基础设施的过程，策略和步骤。

CISO 的主要职责之一是提高应用安全利益相关者的应用安全意识。 在 2012 年由 Ponemon Institute 和 Security Innovation 发起的一项针对包括超过 800 位 IT 高管的调查中，发现 “安全从业者和开发商关于应用安全性成熟度在认知上存在差距，准备和问责制说明为什么许多组织的“关键应用都处于危险之中。” 参加了本次调查开发者中近 80%安全管理人员中的 64%报告他们的组织没有在他们的应用中建立安全控制的过程，超过 50%的开发人员和安全人员报告他们没有获得软件和应用安全的培训，只有 15%的开发人员和 12%的安全人员报告称应用程序满足安全法规，68%的开发商和 47%的官员知道在过去两年里影响应用程序的安全漏洞。很显然，通过安全培训在 SDLC 中构建安全有效率增益的机会。OWASP 有几个培训和宣传资源，可用于应用和软件安全开发、运营和信息安全团队的培训。请参考附录 B ： OWASP 项目和指南在安全培训领域快速参考的更

多信息。

CISO 主要关注的重点是信息安全和风险管理，除了合规性之外的主要要求之一是引入效率和节省在现有的安全过程的开销，包括应用安全的成本。由于信息安全部门分配预算，任何应用安全预算需要满足提高安全性并降低风险。安全和降低风险的目标是通过使用更好的工具和培训开发者以改善安全测试过程。对于大型企业的 CISO，促进软件安全倡议也有满足降低成本，可以通过安全编码标准，安全代码审查，并在 SDLC 的阶段中修复 bug 花费比较少的阶段开展安全测试以降低修复漏洞的成本。请参阅附录 B ： OWASP 项目和指南在帮助 CISO 实现应用程序的安全包括软件开发的安全性和安全性测试过程的信息的快速参考。

CISO 们往往需要通过考虑安全性和业务部门的不同需求来调整应用安全的预算。例如对于服务于金融机构的 CISO，安全性往往是安全计划和业务目标相互妥协的结果。在应用安全计划与业务目标不一致的情况下，对于 CISO 来讲，把重点放在哪里来左，以使应用安全计划与业务目标一致是非常重要的。例如，围绕提高软件的质量和安全性，可以考虑不同的安全选项，以达到安全的情况下降低对客户体验的消极影响。在商业赞助一个新的应用程序开发项目的情况下，CISO 可以以此为契机，为应用程序推动一个的新的应用安全功能，与项目经理一起工作并实现安全标准的合规性，并通过设计和编码来提高安全性，并实现整个项目尚未实现的整体成本的节省。

安全度量的重要性

CISO 的职责是管理应用程序脆弱性风险，安全度量如应用程序脆弱性的度量是构成进行商业案例投资于控制和降低风险应用安全措施的重要因素。在开展应用安全活动过程中，如同一个应用发现的安全漏洞的测量，以降低安全风险和安全漏洞的个数，可以将这些结果展示给高级管理人员和公司高管。采纳应用安全过程，培训和工具，最终能够帮助组织提供漏洞的数量较少和造成组织和客户的风险更小的应用程序和有软件产品。

III-4 确定软件安全活动和 S-SDLC 过程目标

OWASP 为 CISO 提供了几个项目和指导，帮助 CISO 开发和实施软件安全活动和安全的软件生命周期（S-SDLC）。要了解更多，除了阅读本节中的指南，请参考附录 B：OWASP 项目和指南快速参考的更多信息

认识安全软件的重要性和关键性

因为不安全的编码导致了大量的应用漏洞，很重要的是 CISO 能够认识到安全软件在改善应用安全的重要性。不安全的软件可能的原因取决于不同的因素，如编码错误，不遵循安全编码标准和安全要求，引用了有缺陷的软件库，缺少安全代码审查过程和安全测试，缺乏安全编码的培训，或者软件开发人员缺乏安全意识。从 CISO 的角度来看，明白软件安全是一个复杂的学科，需要特别注重安全流程、工具、以及人员技能是很重要的。同样重要的是要认识到，投资于软件安全有助于组织节省在未来的应用漏洞修复费用。通过投资软件安全倡议，组织可以专注于在软件开发生命周期（SDLC）的早期阶段修复漏洞，这比在验证阶段和编码阶段测试解决这些问题花费更少的成本。

现在，也要归功于 OWASP，软件安全已经成熟，并逐渐成为一门学科。例如，一些组织已经在他们的软件开发流程采用软件安全最佳实践，如安全需求文档中，遵从安全编码标准，并使用软件安全测试工具，如静态源代码分析工具，在发布源代码进行构建和集成并最终集成和用户验收测试之前识别源代码中的漏洞。通过在 SDLC 介入软件安全活动，组织可以比不采取这些安全活动生产出的软件和应用具有较少脆弱性和更低的风险。

将风险管理作为 SDLC 的一部分

CISO 可以确定什么样的软件安全活动可以集成为 SDLC 的一部分。根据美国 NIST 发布的 SP800 -30“有效的风险管理必须完全集成到 SDLC... [它]有五个阶段：启动，开发或采购，实施，运行维护和废弃”。把安全整合到 SDLC 过程中首先将识别信息资产，并通过定义保密性，完整性和可用性要求处置软件。接下来的步骤包括信息资产的价值确定，识别潜在威胁和识别所需的应用的安全对策，如身

份验证，授权和加密的。

一套全面的安全要求需要还包括安全一定的安全和技术标准要求，实现安全的软件，安全认可技术平台以及之前与其他供应商的软件组件/库集成软件的安全检查。

采购第三方组件/服务前评估风险

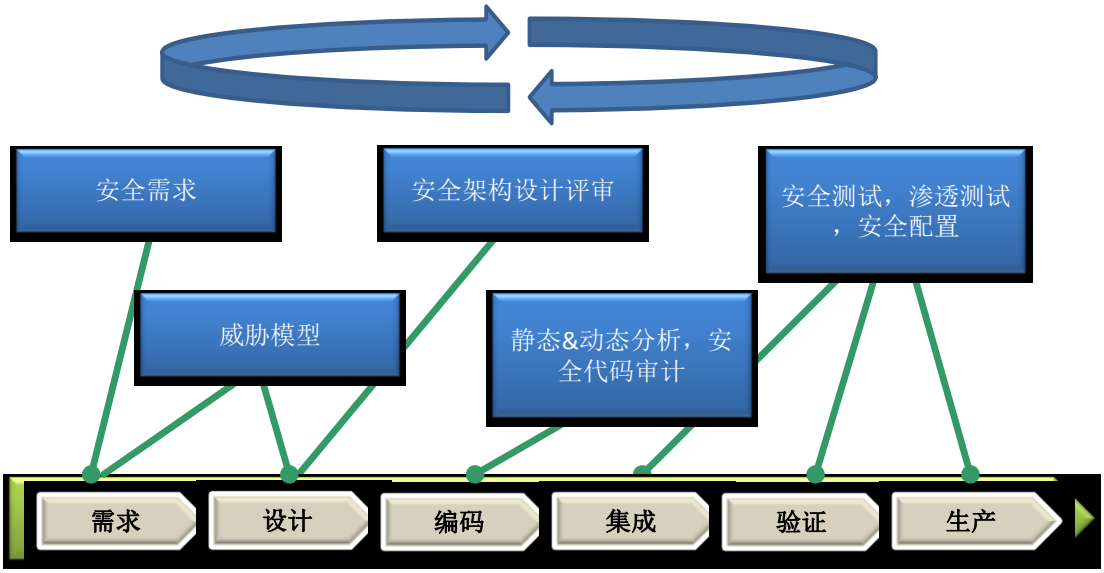
当获取的软件是商用现货供应（COTS）的一部分或作为免费的开源软件（FOSS），对于 CISO 而言，在采用它们之前，针对特定的安全需求用适当的过程来验证这种类型的软件库是很重要的。这可以提供组织 CISO 保证所获取的软件在一定水平上是安全的，并且可以与应用集成。出于这项考虑，OWASP 开发了一个法律项目和包括对生命周期的安全性要求的合同样本附件，使 COTS 产品会比较安全。请参阅附录 B：OWASP 项目和指南快速参考的更多信息，可以帮助 CISO，评估新采购的应用程序，服务，技术和安全工具。

软件开发生命周期（S-SDLC）的安全方法

在有些情况下，组织的 CISO 也有促进组织内的软件安全过程责任，不要对这一目标掉以轻心是很重要的，因为通常认真对待资源的规划和新的流程和活动的开发具有重要意义。好在今天，几个“安全的软件开发生命周期”（S- SDLC）的方法，可以由 CISO 采用纳入安全软件开发生命周期。目前最流行的 S- SDLC 的方法是 Cigital 的触摸点，微软的 SDL ，OWASP 的 CLASP，BITS 的软件保障框架。在较高的水平，这些 S- SDLC 的方法非常相似，包括在整合组织采用的 S-SDLCs 的安全活动，如安全需求，安全体系结构评估，架构风险分析/威胁建模，静态分析/审查源代码，使用组织现有的安全性/渗透测试活动。CISO 从整合 SDLC 的角度来看，他们所面临的挑战是要确保这些软件安全活动与组织使用的软件工程流程一致。这意味着，集成不同类型的 S – SDLCs，如 Agile，RUP，瀑布模型，因为这些可能已经被组织内不同的软件开发团队采用。如何将这些在一个瀑布 SDLC 中集成，以及在一个 SDLC 过程的不同迭代内迭代的例子如下所示。

图 7 内置的瀑布式 SDLC 安全流程实例

安全软件开发生命周期过程（S-SDLC）



通过一种全面的方法对应用和软件的安全性带来更好的结果，因为可以与已经通过组织的信息安全和风险管理相一致。从信息安全的角度来看，对于应用安全的全面方法应包括例如，为软件开发人员以及安全人员和管理人员的安全培训，信息安全和风险管理的整合，信息安全政策和技术标准以及组织使用的信息安全工具和技术杠杆的定位。

软件保证成熟度模型（SAMM）

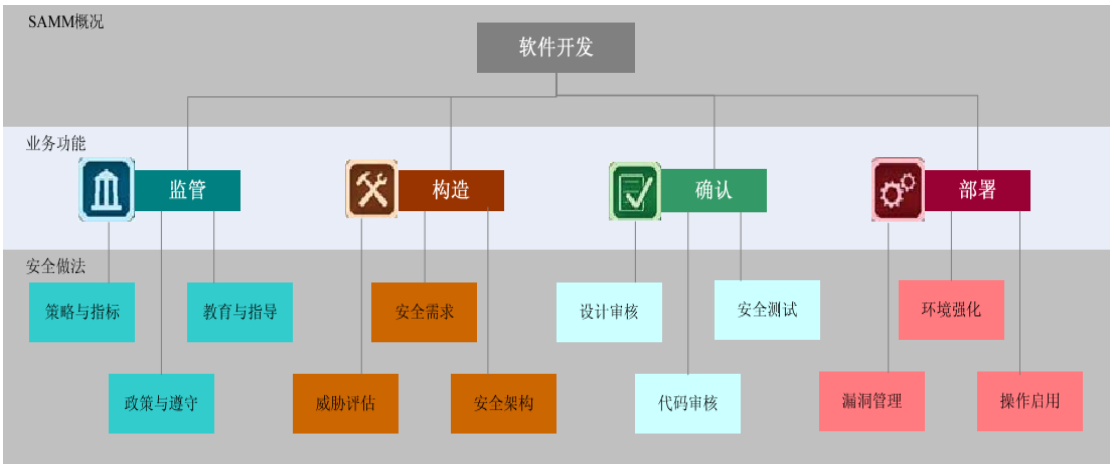
除了遵从一个全面的考虑其他领域的应用安全方法之外，对于 CISO 来说，另外一个也很重要的方面是考虑组织构建软件的安全的能力，并计划如何在未来整合新的活动。今天安全软件成熟度模型使得测量软件安全的组织能力成为可能，如在成熟度模型内构建安全（BSIMM）和开放软件保证成熟度模型（SAMM）。这些模型还可以帮助 CISO 评估，规划和实施本组织的软件安全计划。这些成熟度模型为软件安全保证明确设计。这些模型，即使是基于经验测量，也是真实的数据流入（如软件安全性调查），因此允许测量组织对已实施软件安全计划查看。通过允许其组织的安全软件开发使用这些模型来衡量软件实践，CISO 可以比较其他软件开发组织与组织软件安全开发能力，以确定组织哪些软件安全活动是领先还是落后。

对于组织滞后的软件安全活动，BSIMM 和 SAMM 度量允许 CISO 构建软件安

全活动计划，在未来缩小这些差距。要注意到，这些模型是不是规范很重要，不是告诉组织做什么，而是要衡量与同类组织在这一领域安全活动的对比。这些模型使组织沿着相似的领域，治理，智能，SSDL 触摸点，部署 BSIMM 和治理，施工，验证以及部署 SAMM。SAMM 测量在三个最佳实践和三个层次为各业务功能实现成熟度。

图 8 在开放的软件保证成熟度模型中的业务功能和相关的安全实践

（OWASP 开放 SAMM V1.0）



BSIMM 度量覆盖 12 最佳实践和 110 项软件安全活动。成熟度等级帮助 CISO 规划组织软件安全过程改进。软件安全方面的改进可以通过对每个活动分配的可达的目的和目标进行测量。对于 CISO 而言无论是已经开始部署软件安全计划如组织内的 S-SDLC，或仅仅是将来一个计划，一个度量的模型如 BSIMM 和 SAMM 提供的测量是确定在哪些应用安全活动中重点支出的重要测量指标。如果还不熟悉 BSIMM 和 SAMM，CISO 也可以参照能力成熟度模型（CMM）和各成熟度等级来规划组织安全软件的开发过程能力。

像 BSIMM 和 SAMM ， CMM 也是一个经验模型，其目标是提高可预测性，有效性，和控制一个组织的软件过程。在 CMM 为例，有五个级别可以用来衡量该组织如何区分不同层次的软件工程过程的成熟度：初始，可重复，可定义，可管理，优化。在第一级（初始），组织使用的软件工程过程是临时的和不被控制的。作为软件开发组织到达第 2 级，软件开发过程是可重复的，并可能能够提供一致的结果。当一个组织达到 3 级，这意味着它已经通过了一组严格定义和标准的软件开发流程，这些都是整个组织一贯遵循的。在 4 级，即可管理级，软件开

发组织已采用指标和测量，因此，软件开发可以得到管理和控制。当一个软件开发组织是第 5 级，优化级，重点是通过渐进式技术创新和变革和改进软件开发不断提高改善工艺性能。

谈到软件的安全流程，在 CMM 级别 1（初始）CISO 有一个特设的过程“捕捉”和“修复”应用漏洞。在这一级，组织在软件安全实践的成熟度包括运行的 Web 应用漏洞扫描工具对如验证应用是否符合 PCI-DSS 标准和 OWASP Top 10 事件的反应上。在 CMM 级别 2，该组织已经采用标准流程对应用漏洞进行安全测试，包括现有的软件库和组件的安全代码审查。在这一级，安全测试过程可以重复，以产生一致的结果（例如，如果由不同的测试人员执行得到同样的安全问题），但在相同组织内不是被所有的软件开发群体采用。在 CMM 级别 2，应用程序安全过程也是被动的，也就是说，不执行所要求的安全测试标准。在 CMM 级别 3，应用安全过程遵循定义的流程标准，同一个组织内，所有安全团队都会执行安全过程。在这一级，应用程序的安全也是积极的手段，意思是在产品发布之前，安全测试应用，风险与合规性要求作为治理的一部分被执行。在 CMM 级别 4 （管理），在 SDLC 的不同阶段应用安全风险被识别和管理。在这一级，安全的重点是在产品发布之前消减所有的应用程序的风险。在 CMM 级别 5（优化），应用程序安全过程可以得到不断优化，以增加应用安全活动方面覆盖应用的范围和最高的投资回报率。

安全战略

战略

“战略（希腊“σ τ ρ α τ η γ ί α”- STRATEGIA，“综合艺术，命令，大将”）是一种高层在实现不确定性条件下的一个或多个目标的计划。规划和编组资源为他们最有效和最有效利用的艺术和科学。策略是重要的，因为可实现这些目标的资源通常是有限的。策略也是通过已知的或可能出现的连续开发获得并维持优于对手的位置，而不是致力于在一开始设计的任何具体固定的计划。”

大多数组织应该有一个像普通的 IT 策略的安全策略。它使组织能够超越短期的战术选择和发展战略及长远规划。由于不断变化的网络威胁形势，CISO 为

未来的威胁保护信息资产安全是很重要的。这种策略可以指导经营决策，计划和确定重点资源投资的适当水平，以实现组织的目标。

建立一个计划，并准备改变它

安全策略不会涵盖所有的可能性，而是为你提供一个良好的战略框架。此外，随着时间的推移你的环境或相关假设会发生变化，你的策略将需要不断的改进，并作相应调整。定义一个策略并经常修改它是更好的选择，使其适应新的环境，而不是无限期地发展你的安全策略，等待所有的信息变得可用。

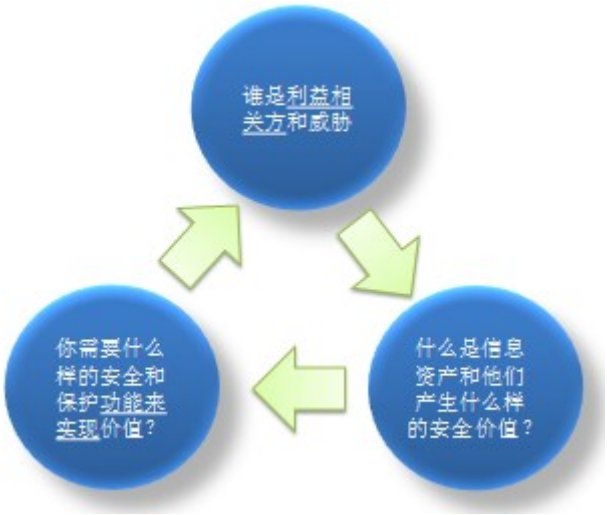
要定义你的安全策略的基本原理，你应该考虑以下三个一般问题：

1. 利益相关者：谁是你的主要利益相关者和潜在的威胁代理？

2. 资产：什么是您的信息资产，以及它们如何（他们的保护）在你的客户组织内部和外部创造价值？

3. 功能：什么是该组织及其利益相关者需要提供的价值定位的重要的安全和保护功能？

图 9 安全战略三个关键问题



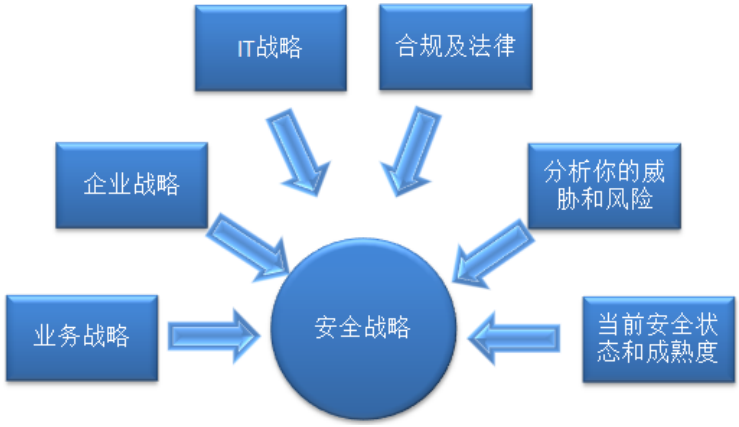
如何定义组织的安全战略

如同所有的战略文件你将分析的基本假设和目标的影响，并得出对如何达到这些目标的安全策略。

收集输入用于开发您的安全战略

一般情况下投入是定义你的安全策略的过程非常有用。通常组织可能没有所有输入或这些输入可能在非正规少访问的状态（例如在某些组织中拟的关键员工的头脑）。或者，他们可能会过时或不完全匹配你所期待的。制定一个基于有限清晰的组织总体战略或缺少部分信息的安全策略可能具有挑战性。但是，，最好还是随着时间的推移开发一些策略和随着越来越多的相关信息变得可用不断改进它。

图 10 开发安全战略输入



1. 业务战略

CISO 应该首先看该组织的业务战略，例如任务书，业务目标以及为支持这些目标的其他策略组件（参见以下各点）。例如，其中的操作部分依赖机密性，可用性和由 IT 职能所提供的信息的完整性的程度多大？在发生系统故障或信息泄密的情况下，对销售和市场营销的影响是什么，如何依赖 IT 骨干网上的供应链，可以在失败的情况下交付，在安全问题产生的时候欺骗行为能够被发现？哪部分价值链更容易受到潜在的攻击？哪些机会可以在一定的安全情形下作为企业的竞争优势（如更强大的安全环境，使能够提供更多的电子商务，更高的依赖 IT 流程和更高的效率）？可以使采购过程发生巨大变化，如允许 BYOD（带上你自己的设备）的策略？是否有新的和具有潜在破坏性的商业案例可能的，因为安全和可靠的应用程序？你在多大程度上可以让你的一些数据，脱离您的组织的直接控制（如在基于云的应用程序）？你怎么能最大限度地减少风险，通过法律和技术控制？由此导致的结果对于业务来讲是否是可接受的风险？

2. 企业战略

你的企业战略如何与 IT 和安全策略是否相一致？请问贵公司组织结构是专门做分散还是集中？这将如何影响加强中央和地方的安全策略的能力？频繁的企业并购和整合的企业战略以及如何有效地整合新的实体和管理整个组织这些新收购的公司实体的安全性重要组成部分？

3. IT 架构的 IT 战略＆评价

安全战略的一个重要方面是依赖于系统是否分散或集中的 IT 战略，例如：调整，这将决定如何以及在延伸机构可以强制执行中央和地方的安全策略。其他方面是系统架构概述，信任边界，数据流，传输过程中的数据，以及剩余的数据。您的业务战略是如何驱动你的 IT 战略。贵组织有什么样的 IT 资产以及计划继续向前迈进能力？

4. 合规及法律要求

5. 分析你的威胁和风险

你需要了解这些风险是如何影响您的业务运行，并可能影响您的业务和经营战略。 （另见本指南第 2 部分）

6. 评价您目前的安全状态

设置安全策略之前，需要考虑的另一个重要因素是组织中的各个安全域的功能和具体应用安全领域的成熟。CISO 可以使用成熟度模型如 OWASP openSAMM 和各种活动的战略和度量（SM）来查看当前的安全状态，并设定目标。具体而言，依据 openSAMM 模型，CISO 可以从 1 级（基本）SAMM 活动，诸如如“评估整体业务风险”和“建立和维护保证计划路线图”开始。随着组织的成熟度的增加，CISO 可以将 2 级 openSAMM 活动，如“根据业务风险分类数据和应用程序”，以及“建立并测量每个分类的安全目标”并入。了解你的组织目前的安全状态将允许开发一个清晰的路线图，作为一个良好的安全策略的关键部件之一向前迈进。

你的安全策略的组成部分

安全策略应包含或启用下列组件：

1. 总的指导原则和重点

组织在未来的 X 个月有什么安全的投资。一般情况下大多数公司都使用时间周期 12 - 24 个月的策略定义。有一个定义为 12 个月的主要安全策略是恰当的，同时第二个更长远的 2 年和 5 年的规划，具体取决于组织的类型，概述了较长期的安全投资计划。当然，在当今快速变化的安全空间，威胁和风险非常迅速地改变，计划也应该随着相关假设的变化进行调整，并至少每年进行审查。

2. 风险管理，风险接受水平

（见第二部分）

3. 安全路线图

要定义您的安全路线图，一个很好的方法是看一般的公司的安全路线图和从基于使用例如像 openSAMM 成熟度模型结合风险评估得出的安全路线图。

4. 安全架构和流程

什么样的安全特性性能代表整体系统架构？哪些地方是你的组织的信任边界和基本信任假设？哪些是核心安全系统如身份验证和授权？本地系统与个别中央系统有多深的依赖程度等，如部署单点登录或等效的方案，中央系统管理所有的授权控制有多可靠？

此外，该安全架构需要考虑的攻击面和网络威胁风险，特别是其中的应用架构和功能的部分很容易受到潜在的网络攻击。以及架设的灵活性，因此，问题是哪个安全体系架构在承受攻击的情况下最有弹性，例如 DDoS。

安全技术和服务的采购也是安全战略的重要组成部分。问题要问采购过程是否涉及通过采用第三方技术和哪些组织可以做，以提高第三方流程和应用安全引入安全风险。

在今天基于云的系统中，数据往往可以通过网络（如在云中）和系统流离开安全范围。该组织可能没有或者只有在这些数据的保护，在这样的云应用的控制非常有限。

5. 商业及事件响应的连续性

重要的是，CISO 同时开发一个业务连续性（COB）计划的安全战略，考虑到可能的系统故障和运作 IT 基础设施供应链的依赖关系的一部分是很重要的。

安全策略应该提前考虑最坏的情况和计划的安全措施。积极主动的风险策略是回答有关管理业务影响事件实际出现前的问题。例如对于一个服务交付业务的

问题可能是应用是否仍然可以运作，以确保发送和安全失败。

图 11 安全战略要素

结论

对于安全战略的总体目标是尽量减少风险，最大限度地为组织带来商业利益。该战略必须回答的关键问题是是否应用了安全措施后，安全控制是足够的，高效的足以减少对组织风险和剩余风险对于业务是可以接受的。

图 12 应用安全路线持续期分析

（OWASP CISO 2013 年调查）

持续期	%
1 年	35.59%
2 年	28.81%
3 个月	10.17%
3 年	10.17%
5 年以上	6.78%
6 个月	8.47%
累计	100.00%

一般来说，大多数的路线图持续时间是 1-2 年的。 2013 年 OWASP CISO 调查发现，64％的路线图计划为 1-2 年。

III-5 如何为您的组织选择合适的 OWASP 项目

整体安全水平和风险配置文件的组织单元可以根据不同的工具和标准对 CISO 推动他或她的安全战略尤其有用。

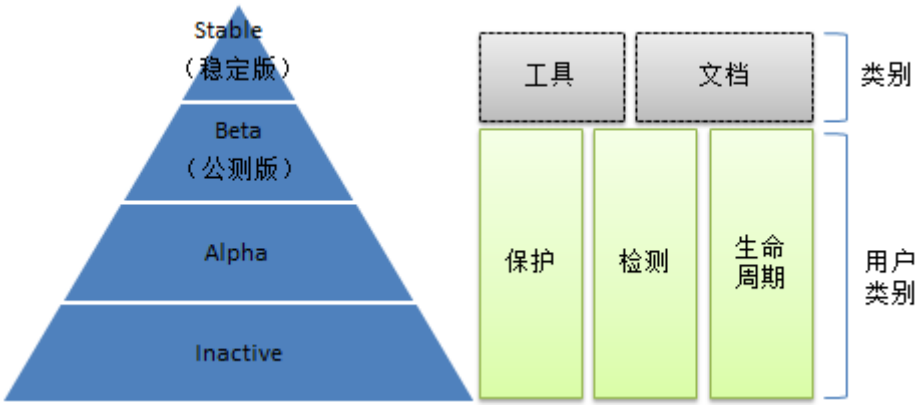
请注意，前面的章节中讨论的风险，根据不同业务部门的风险状况，安全策略实际上可以根据各自不同风险情况和不同监管要求而不同。例如，财务部门可能需要大幅走强的安全状态，而内部网页公布餐厅午餐菜单的基本安全措施可能要得到充分保护。（不过在军事设定的提交知识，即使是午餐菜单页可能被视为机密信息，从供应物流也可以派生出进一步的信息）。

基于这些不同风险程度不同工具和标准与有关项目和组织单元更相关。

还要注意的是 OWASP 提供了几个项目和指导，帮助 CISO 在软件安全发展和安全测试流程的制定和实施提供帮助。请参阅附录 B： OWASP 指南和项目的快速参考。

一般的工具可以分为不同的类别（所以也是 OWASP 的项目）。

图 13 图解 OWASP 项目类别



项目的成熟度

- Stable（一个成熟和不断维护的项目或工具并得到良好的质量）
- Beta（相对成熟，虽然不是最佳质量）
- Alpha（这通常体现了良好的第一个原型，但仍然有很多功能可能缺失或达不到标准）
- Inactive（已退役或废弃，或在以前某个时候已经放弃了的项目）

显然，对于 CISO，最感兴趣的是稳定和可靠的项目和工具。在未来的日子里，一定程度上他可以依靠某种成熟的品质并使用和维护。Beta 项目也可以是非常有价值的，因为他们可能代表还没有完成其全部审查周期，但已经可以提供尝鲜试用，可以帮助你为你的安全程序和工具建立良好的基础并向前发展。

项目的类别

通常 OWASP 项目被分为两种：工具或文档。并通过使用类别：建设者，破坏者和维护者。这些类别可以帮助管理者通过快速导航获得更多的组合，在 OWASP 提供的工具中更容易找到他目前需要的合适项目。

人员，流程和技术

CISO 也可以选择通过三种主要方式来实现自己的安全目标。人员、流程和技术。管理组织这个通常是很重要的三大支柱，实现整个组织最佳影响的塑造。如果仅仅把重点放在一个或两个方面，他们可能使组织受到伤害。

图 14 人、流程和技术控制支持应用安全

人

这将解决员工、供应商、客户和合作伙伴的培训和激励。如果他们受过良好的教育和激励，恶意行为或意外失误的概率可以大大降低，可以避免许多基础的安全威胁。

流程

如果一个组织变得更加成熟，该流程将被明确界定，并在事实上以“正确的方式”做事。流程可以确保组织的行动变得可靠和可重复的。例如具有良好定义的标准作业程序，事件响应过程将是可靠的，不依赖于临时的决定，不受各种不同的个别决策者特设的决定的影响。在高度成熟的组织，业务和 IT 流程将不断评估和改进。如果故障发生，改善流程可以让一个组织作为一个整体从过去的错

误中吸取教训并改进其运作，使其以更高效，更安全的方式运行。

技术

技术可以引导和支持人员提供良好的培训和知识为配合和推动工作。技术可以促进组织遵循良好的安全实践提供良好的工具，同时使其难以从正确的道路偏离而不被发现。例如，好的技术会自动完成访问控制和认证，使他们的授权用户非常简单的使用，同时可以拒绝未经授权或特权访问的攻击。最后，一些自动化的工具可以在后台帮助和支持人员和组织对他们工作上的风险进行更有效，更高效地防守。许多安全标准和工具（在 OWASP 和其他机构）也可以看作是着眼于该框架的一部分。例如，员工培训可以使人员建立自己对安全的理解和做正确的事，而各种 SDLC 的模型可以帮助企业建立它的开发和事件响应机制流程的适当的水平。

（翻译 贺新朋）

第四部分：管理风险及应用安全投资度量

IV-1 内容提要

CISOs需要指标向高级管理层报告应用程序安全计划投资的有效性及其对业务风险的影响。CISOs也需要指标来管理和监控组成应用程序安全计划的人,流程和技术。

这些衡量指标由三种类型组成。CISO们应该能够在回答这些问题的基础上度量和推动他的团队通过自动化工具在一个近乎实时的基础上进行。关键问题包括：

- 应用安全流程指标 - 该组织如何很好地满足安全策略、技术标准和行业惯例？我们如何贯彻执行安全SLA？是通过应用程序、按部门划分还是按渠道？
- 应用安全风险指标
  - 脆弱性风险管理指标 - 什么是年度平均修复时间（MTTR）？按月？通过应用程序？按部门划分？哪些是生产过程中已知的安全问题？
  - 安全事故指标 - 哪些安全问题已被识别？在被公布的生产问题哪些

是已经被利用者知道的？什么是业务成本？

- 威胁情报报告和攻击监控指标- 哪些应用正在接受比其他更多的攻击？即将到来的预期峰值的应用使用情况如何？

- 软件开发生命周期的安全指标
  - 度量风险缓解的决策- 应用风险类别平均修复时间(MTTR)是什么？它是否达到预期？什么是应用风险热度图？按部门划分还是渠道？
  - 脆弱性根源识别度量 – 每个应用漏洞的根源是什么？有没有系统性问题？每个开发团队已经采用哪些最佳安全实践？哪些开发团队需要更多的关注？
  - 软件安全投资度量 - SDLC阶段已识别哪些主要安全问题？什么是在每个SDLC阶段相应的安全实践的成熟度？在每个SDLC阶段迫切需要更多的安全人员，流程和技术是什么？

注：OWASP 提供了一些项目和指导用于帮助 CISO 们度量应用资产监控安全和风险在组织内开发和实施应用安全性计划。除了阅读本节中的指南，请参考《附录 B：OWASP 手册及项目快速参考》中应用程序风险管理指标和监控领域 OWASP 项目的详细信息。

IV-2 简介

这部分指南的目的是帮助CISO们管理应用安全计划的诸多方面 - 特别是风险和法规遵从，以及应用的安全性资源，如流程，人员和工具。其中一个应用的安全性度量的目标是测量应用安全风险以及信息安全的法律，法规和标准在应用安全需求合规性。其中的CISO们需要报告和管理关键应用安全流程中开发流程和操作等方面的应用漏洞管理。给高级管理层报告应用安全活动的状态等等往往是CISO们的责任，例如：应用安全测试和软件安全活动在SDLC的地位。

从风险管理的角度来看，重要的是应用安全度量包括的技术风险，例如针对组织开发和管理应用没有缓解的漏洞的报告。这些度量的另一个重要方面是测量范围，如在应用安全验证计划中应用组合定期评估的百分比；内部应用与外部应用涉及的百分比；以及当他们执行SDLC时这些应用和进行安全评估的类型的固有风险。这些类型的度量帮助CISO们向信息安全负责人以及企业主报告应用安

全过程的符合性和应用安全风险。

由于 CISO 的职责之一是管理信息安全和应用安全风险，并就如何减轻他们做出决定，通过这些重要的度量标准以便能够衡量集中于组织资产的风险，包括应用程序数据和功能。

IV-3 应用安全流程度量

度量和测量目标

应用安全过程度量的目标是确定组织的应用安全流程如何很好地满足了应用安全策略和技术标准规定的安全要求。例如，一个应用漏洞处理可能包括要求面向互联网的应用每六个月或十二个月根据应用的固有风险评级执行漏洞评估。另一个漏洞处理要求是要在多个SDLC过程中，如：体系结构风险分析/威胁建模，静态源代码分析/安全代码审查和如面向公民、客户、顾客、员工等存储个人敏感信息的关键服务的应用程序的安全执行基于风险的测试等等。

从流程覆盖范围的角度来看，这些度量的目标之一可能是报告如应用安全过程的覆盖面，以衡量应用程序如何进入应用安全评估范围，以找出基于应用类型的潜在漏洞评估差距和应用安全需求。这些帮助CISO们提供过程覆盖范围可见性以及应用安全计划的操作执行状态。例如，度量标准可能会显示（例如红色的状态），应用安全过程在SDLC中如安全代码审计一定数量高风险评分的应用和标记没有被执行安全测试要求而导致的不合规的问题。这种类型的度量允许CISO根据流程要求优先为最需要符合标准的过程分配资源。

为应用安全验证的另一个重要测量是测量当应用安全过程计划与实际执行时识别安全代码审查、静态源代码分析、道德黑客与应用渗透测试过程中的潜在延迟。

IV-4 应用安全风险度量

脆弱性风险管理指标

CISO们的职责包括对应用安全风险的管理。从技术风险的角度看，应用安

全风险可能是由于应用漏洞暴露如：数据和关键功能，以寻求得以入侵这些应用资产的潜在攻击。

通常情况下，技术风险管理还包括缓解风险所构成的应用补丁和漏洞对策。这些漏洞的风险的缓解通常是优先考虑基于风险的定性测量。例如，组织在每个应用开发和管理中会有一定数量的以确定的安全漏洞按严重性排名（如：高、中、低）。高风险和中风险漏洞数量越多，应用的风险越高。数据资产保护的应用和支持功能的关键性价值越高，这些漏洞对应用资产的影响越高。

脆弱性度量中的一个重要的数据点是仍未修复的安全漏洞的数量。一个给定数量的应用漏洞可能仍然是“开放”的，即在不固定生产环境下和给组织带来的这些风险，需要 CISO 优先考虑的风险缓解措施，如“关闭”中的漏洞可以被视为可接受的应用的漏洞管理标准符合性框架。

安全事件度量

对于CISO管理信息安全风险的另一个重要指标是有关由组织开发和/或管理应用安全事故报告。CISO可以收集来自SIRT（安全事件响应团队）这些数据报告由于漏洞的利用给特定的应用带来的影响。对于一个给定应用安全测试漏洞报告与安全事件报告的相关性使得CISO优先减少可能导致企业影响最大的漏洞努力缓解风险

显然，通过等待安全事故的发生来决定有针对性的缓解漏洞的反应，而不是主动的对风险的管理方法，但反馈是非常重要的。

威胁情报报告和攻击监控指标

主动面对风险的组织不要等安全事故的发生，而是从其他攻击、已发布的漏洞和安全威胁情报中学习，利用这些信息从而调整风险级别和风险评估，采取主动的风险缓解措施，例如，制定和实施对策或者优先安排缓解已知的被利用后可能会在事件中造成最大影响本组织的漏洞。CISO可以使用威胁情报报告，以及从监控应用层的安全事件，如从SIEM系统 （安全信息和事件管理系统）和蜜罐应用度量风险评估水平。不幸的是今天，大多数的安全事故被发现和报告后仅几个月入侵或数据泄漏成为现实。可操作的安全度量和有针对性预防攻击的风险对

于CISO们至关重要，因为它可能有助于决定哪些应用要放在更严格的监视和警报下，以便能够更快地在遭受攻击时能法降低事件的影响。例如，：

- 一个可能的针对网上银行应用分布式拒绝服务攻击（DDoS）的威胁警报可能允许CISO为组织建立预警准备和对策，以防止随后造成的中断
- 恶意软件针对电子商务应用窃取用户凭据并进行未授权购买的威胁报告让CIS0发出事故事件监控管理团队监控警报。

已发布的软件框架或库中的漏洞可能会改变 CISO 安排的修补程序测试、部署和验证。

IV-5 安全在 SDLC 管理度量

风险缓解决策的度量

一旦漏洞在开发和操作的任何阶段确定，接下来的步骤是决定其应该其修复的时间和方式。漏洞评估过程合规性需求可以用来解答第一个问题，漏洞评估过程合规性需求可能状态例如高风险漏洞被修复在较短的时间框架中、低风险漏洞。。该需求还可能根据应用的类型的变化而变化，例如：一个完全新开发的应用与现有应用的新版本之间。随着新的应用先前没有安全性测试，代表他们比现有应用的风险更高，因此，这可能需要发布的应用进入生产前高风险漏洞被消减。一旦问题被识别并依据漏洞的风险程度优先缓解，下一步就是确定如何修复漏洞。

这取决于多种因素，如漏洞类型、受此漏洞的影响最有可能被引入的安全控制/措施。这种类型的度量允许 CISO 确定漏洞的根源，应用开发团队根据情况提出补救措施。

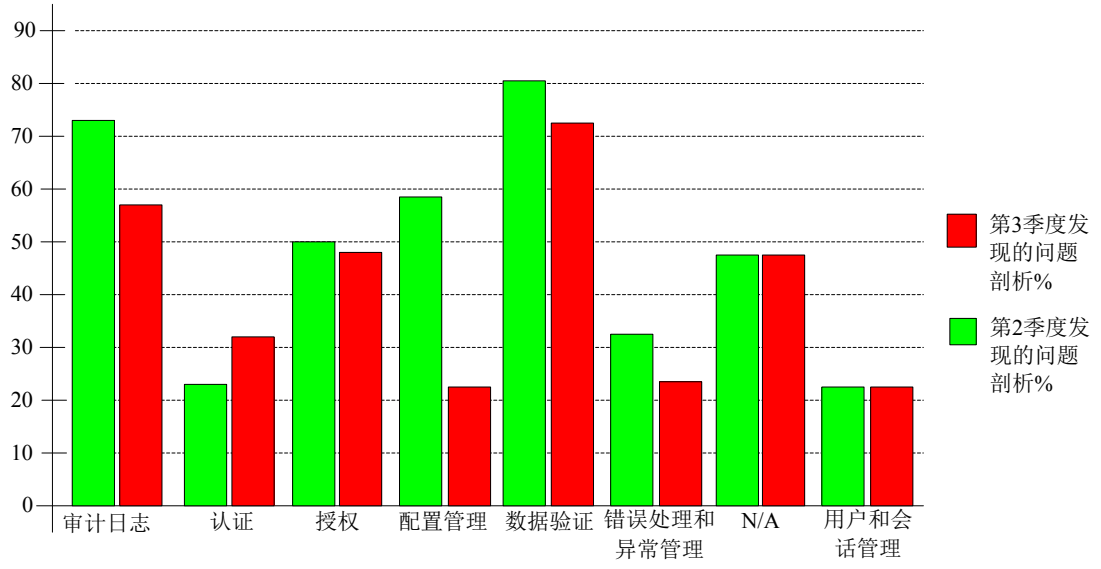
脆弱性根源识别的度量

常态化的漏洞度量报告可以让CISO们通过评估来改善。例如，测量一段时间内同一应用类型的单个问题的情况，有可能为CISO指出潜在根源。用漏洞度量趋势分析和漏洞类型分类，可能为CISO建立基于特定类型的安全活动商业投资，如流程改进、采用测试工具以及培训和宣传。例如，在图1显示度量中，通过比较相同的应用2季度版本显示了若干类型的漏洞的良好发展趋势。应用安全

改进测量如：从一季度发布到另外一个确定可以观察大部分漏洞类型的漏洞数量减少，除了认证和用户/会话管理问题。

CISO 们可以使用这些度量标准，与 CIO 和开发董事讨论随着时间的推移组织应用软件发布安全状态是否是在恶化还是改善，并引导应用安全的资源（如：过程、人员和工具）在哪里更需要降低风险。例如，在图 1 度量显示，假设发行版本之间引入了应用程序的更改不会有太大的类型和复杂性来看，以及在开发团队中软件开发者的数量和类型及所使用的工具，这种情况下，可以专注对组织的问题的类型进行修复漏洞，如更好的设计和实现身份验证和用户/会话管理控制。然后 CISO 可以与 CIO 和开发董事协调来安排这些类型的漏洞、认证和会话管理文档开发指南进行有针对性的进行培训，并采用特定的安全测试案例。最终，这些协调的努力将授权软件开发商在设计、实现和测试更安全的身份验证会话管理控制并作为改进脆弱性指标的表现。

图 15 漏洞分类趋势图



软件的安全投资的度量

S-SDLC安全度量的另一个重要方面是SDLC要决定从哪里开始安全性测试和修复投资。要知道这一点来衡量它是很重要的，这是软件开发生命周期中最脆弱的（问题的比例最高）的源头，这些漏洞进行测试和组织在软件开发生命周期（SDLC）各个阶段修复它们需要多少成本。衡量这种根据对测试和管理软件bug（参考Capers Jones研究）成本示例图中的度量示例。

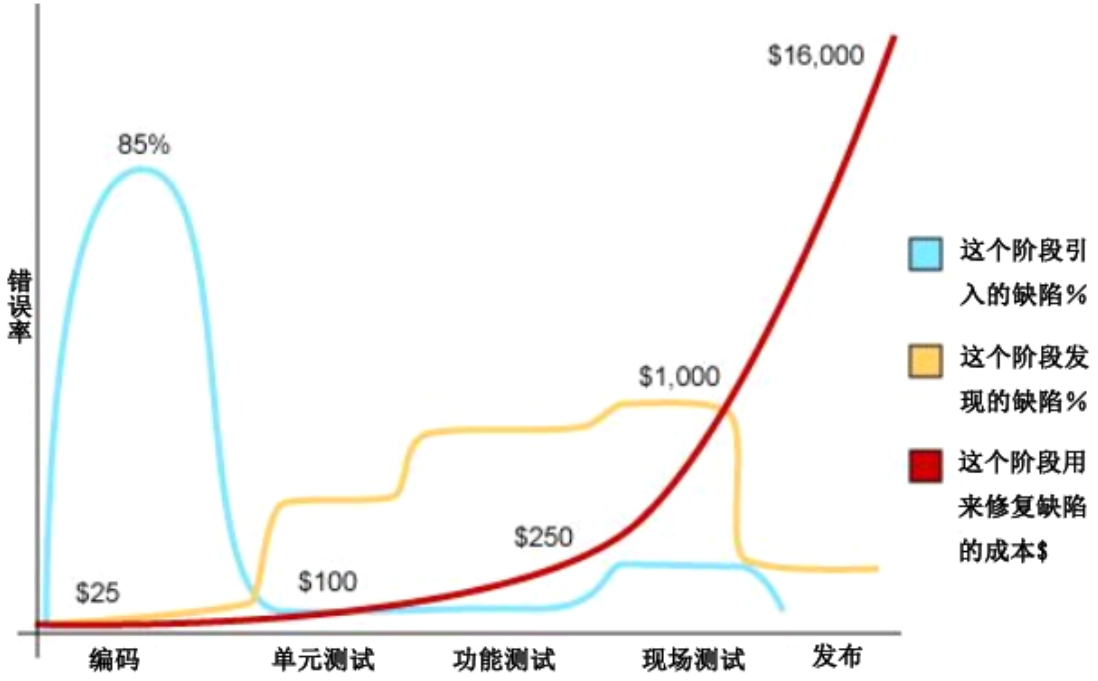
这些量度也可用于辅助应用和基础设施之间的安全投资的适当分配。

通过相似类型的安全缺陷管理度量可以使CISO降低整体安全成本，有效管理安全性问题。假如CISO已经使安全性贯穿整个SDLC过程，并已经拨出预算投资在安全软件开发生命周期活动，如安全编码培训和安全代码审查过程以及静态代码分析工具，这些度量可以让CISO在软件开发生命周期的早期阶段建立测试和修复安全问题的投资计划。这个案例研究是基于以下测量结果：

- 大多数漏洞是由软件开发人员在编码过程中引入
- 这些漏洞的现场测试大多数应该在生产前进行测试，并
- 在软件开发生命周期后期测试和修复漏洞是最没有效率的方式，因为在生产前测试比在单元测试过程解决问题大约要多10倍的价钱

CISO 们在做出安全的软件开发活动投资时，可以使用类似这些漏洞案例研究或者使用自己的度量标准，因为这会节省企业的时间和金钱。

图 16 图说明测试和管理软件 bug 的费用与 SDLC 阶段有哪些不同



（樊山）

支持信息

参考文献

度量和基准

报告发布日期.

2013

- 2013Verizon数据泄露调查报告: http://www.verizonenterprise.com/DBIR/2013/
- Security Innovation and the Ponemon Institute: The Current(2013) State of Application Security report: https://www.securityinnovation.com/security-lab/our-research/current-state-of-applicationsecurity.html

2012

- Security Innovation and Ponemon Institute's 2012 Application Security Gap Study: A Survey of IT Security & Developers: https://www.securityinnovation.com/uploads/Application%20Security%20Gap%20Report.pdf

2011

- Verizon 2011 Data Breach Investigation Report: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report2011_en_xg.pdf
- US Q2 2011 GDP Report Is Bad News for the US Tech Sector, But With Some Silver Linings: http://blogs.forrester.com/andrew_bartels/11-07-29-us_q2_2011_gdp_report_is_bad_news_for_the_us_tech_sector_but_with_some_silver_linings
- Imperva's July 2011 Web Application Attack Report: http://www.imperva.com/docs/HII_Web_Application_Attack_Report_Ed1.pdf

2010

- First Annual Cost of Cyber Crime Study Benchmark Study of U.S. Companies, Sponsored by ArcSight Independently conducted by Ponemon Institute LLC,

July 2010:
http://www.arcsight.com/collateral/whitepapers/Ponemon_Cost_of_Cyber_Crime_study_2010.pdf

- 2010 Annual Study: U.S. Cost of a Data Breach:
http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach

2009 and prior

- OWASP Security Spending Benchmarks Project Report:
https://www.owasp.org/images/b/b2/OWASP_SSB_Project_Report_March_2009.pdf
- Identity Theft Survey Report, Federal Trade Commission,September, 2003:
http://www.ftc.gov/os/2003/09/synovatereport.pdf

标准

- PCI DSS:
https://www.pcisecuritystandards.org/security_standards/index.php
- OWASP Application Security Verification Standard
https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

准则和最佳做法

- OWASP Top Ten:
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- Supplement to Authentication in an Internet Banking Environment:
http://www.fdic.gov/news/news/press/2011/pr11111a.pdf
- Feiman, Joseph. Teleconference on Application Security. 9 Oct. 2008. Gartner. 30 Sept. 2013
http://www.gartner.com/it/content/760400/760421/ks_sd_oct.pdf

安全事件和数据泄露

- Data Loss Database:

http://datalossdb.org/

- WHID, Web Hacking Incident Database: http://projects.webappsec.org/w/page/13246995/Web-Hacking-Incident-Database
- Sony data breach could be most expensive ever: http://www.csmonitor.com/Business/2011/0503/Sony-data-breach-could-be-most-expensive-ever
- Dmitri Alperovitch, Vice President, Threat Research, McAfee, Revealed: Operation Shady RAT: http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf
- Health Net discloses loss of data to 1.9 million customers: http://www.computerworld.com/s/article/9214600/Health_Net_discloses_loss_of_data_to_1.9_million_customers
- Albert Gonzalez data breach indictment: http://www.wired.com/images_blogs/threatlevel/2009/08/gonzalez.pdf
- Share prices and data breaches: http://www.securityninja.co.uk/data-loss/share-prices-and-databreaches/
- EMC spends $66 million to clean up RSA SecureID mess: http://www.infosecurityus.com/view/19826/emc-spends-66-million-to-clean-up-rsa-secureid-mess/

安全性投资和预算

- Gordon, L.A. and Loeb, M.P. "The economics of information security investment", ACM Transactions on Information and Systems Security, Vol.5, No.4, pp.438-457, 2002.
- Total Cost of Ownership: http://en.wikipedia.org/wiki/Total_cost_of_ownership
- Wes SonnenReich, Return of Security Investment, Practical Quantitative Model: http://www.infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf
- Tangible ROI through Secure Software Engineering: http://www.mudynamics.com/assets/files/Tangible%20ROI%20Secure%20S

W%20Engineering.pdf

- The Privacy Dividend: the business case for investing in proactive privacy protection, Information Commissioner's Office, UK, 2009: http://www.ico.gov.uk/news/current_topics/privacy_dividend.aspx
- A commissioned study conducted by Forrester Consulting on behalf of VeriSign: DDoS: A Threat You Can't Afford To Ignore: http://www.verisigninc.com/assets/whitepaper-ddos-threatforrester.pdf
- The Security Threat/Budget Paradox: http://www.verizonbusiness.com/Thinkforward/blog/?postid=164
- Security and the Software Development Lifecycle: Secure at the Source, Aberdeen Group, 2011 http://www.aberdeen.com/Aberdeen-Library/6983/RA-software-development-lifecycle.aspx
- State of Application Security - Immature Practices Fuel Inefficiencies, But Positive ROI Is Attainable, Forrester Consulting, 2011 http://www.microsoft.com/downloads/en/details.aspx?FamilyID=813810f9-2a8e-4cbf-bd8f1b0aca7af61d&displaylang=en
- Dan E Geer Economics and Strategies of Data Security: http://www.amazon.com/Economics-Strategies-Data-Security-DANIEL/dp/B001LZM1BY

关于 OWASP

描述

OWASP 是一个可以信任的全球性开放社区，致力于帮助企业开发，采购和维护应用软件。OWASP 建立文档、工具、教学环境、指导方针、检查表和其他材料，以帮助企业改善他们能力以便开发安全的代码。OWASP 所有的工具、文档、论坛和分会都是免费开放给任何有兴趣改善应用安全的人员。

OWASP 成立于 2001 年，当一群安全专家逐渐意识到，我们开发的 Web 应用方式是多么的可怕不安全时，以完全有组织的方式成立。最初的目标被认为适度的：为开发人员提供编写指南，其中包括软件安全开发实践文档。尽管最初的努力持续几个星期生成出来长达数百页的文档。在发布《构建安全的 Web 应用

OWASP 指南》获得成功后，OWASP 指南陆续发布六个文件。

OWASP 聚集了一个地方良好的人员，帮助提高应用软件中的安全性问题的认识。这是一个基础性的工作，他的驱动力来自于每天都在处理这些问题并想伸出援助之手使情况变得更好的人。OWASP 基金会是确保项目的长期成功的一个非营利性实体。

参与

欢迎大家参加我们的论坛、项目、分会和会议。OWASP 是学习应用安全到网络，甚至使您获得专家声誉的一个奇妙地方。所有 OWASP 的文件、工具和其他资源使用开源许可证发布，并且免费提供的。

各地分会

OWASP 在世界各地有近 200 个地方分会。分会会议都是免费参加，在每个分会的 Web 页面提供免费的演示文档和中立的供应商。这些会议有助于促进世界各地在本地讨论应用安全。

要了解如何启动一个新的离你最近的地方分会、信息以及如何运行一个分会请查看

https://www.owasp.org/index.php/OWASP_Chapter

https://www.owasp.org/index.php/Chapter_Leader_Handbook

应用安全会议

在过去的十几年，OWASP APPSEC 会议汇集业界、政府、安全研究人员和从业者讨论本领域的应用安全的状态。全球 APPSEC 会议每年在北美、拉丁美洲、欧洲和亚太地区举办一届。此外，区域性活动均在诸如巴西、中国、印度、爱尔兰、以色列和华盛顿特区等地进行，每次会议后演示幻灯片和录像在 OWASP 网站上免费提供。

对于即将到来的全球性和区域性活动见

https://www.owasp.org/index.php/Category:OWASP_AppSec_Conference

参考文献

这里可以发现几乎 80 个国家和国际立法、标准、准则和引用 OWASP 委员会和行业规范见 https://www.owasp.org/index.php/Industry:Citations

帮助支持 OWASP 的使命

许多组织已经成为公司或教育的支持者。更有无数组织鼓励员工贡献时间和资源支持 OWASP 项目。

OWASP 还为其他团体产生了六项指导文件，提示他们如何能最好地支持 OWASP 的使命。这些就是所谓为政府机构、教育机构、标准组织、行业组织、认证机构和开发机构的 OWASP 应用安全代码指南。代码指南可以从项目页面下载 https://www.owasp.org/index.php/OWASP_Codes_of_Conduct

联系

全球通讯地址

FAO Kate Hartmann OWASP Foundation 1200-C Agora Drive, #232 Bel Air, MD 21014 United States

欧洲区通讯地址

OWASP Europe VZW Leinstraat 104A B-9660 Opbrakel Belgium

或电话Kate Hartmann：+1301-275-9403或使用在http://sl.owasp.org/contactus的联系表格

CISO 指南附录

附录 A：数据与事件成本的价值

介绍

这个快速参考是在组织由于安全事件导致有关资产丢失后如何通过分配货币价值给信息资产以确定导致的货币影响提供指导。

本附录中也包括一个简单的公式来确定数据丢失的情况下事件的潜在责任风险和基于统计数据的数据泄漏计算工具来估算数据泄露的本。

信息的价值

安全措施的选择必须考虑资产被保护的价值。所有类型的数据可以从不同角度来确定价值，如个人数据。其作为一种资产，虽然可能是最普遍被看到的数据，它的价值作为组织或事件的成本，这些既不总是最合适的，也不是通过最大化的估值来考虑。例如，看个人资料（个人身份信息）报告的价值建议从四个角度绘制其个人信息隐私的价值。它们是：

- 其作为该组织的业务中使用的资产的价值
- 其所关乎个人的价值
- 其他各方谁可能要使用的信息的价值，无论是合法或不正当的目的
- 监管机构和其他团体所解释的社会价值。

数据主体的一方或者社会的价值比其他人更适合某些组织。该报告还分析未保障（个人）数据和保护中受益之间带来的更广泛的影响。它描述了涉及个人数据导致金融诈骗的事件，如何对个人带来更大的影响，但财务影响并非唯一的影响。该报告提供计算方法，并提供了示例，在 2008 年其中一个人的个人资料数据的值可以在 500 - £1,100（大约$800 - $1,800）。

数据破坏和经济损失

对于每个受害者财务上的损失具体数字被认为取决于不同行业类型和攻击

造成数据丢失事件的类型等因素来计算。据 Ponemon 研究所在 2010 年 7 月有关不同行业 45 个组织进行的网络攻击成本研究中表明，基于 Web 攻击的成本是年度网络攻击成本的 17%。在不同的行业该成本随国防，能源和金融服务（16310000 美元，15630000 美元和 12370000 美元分别）比组织在零售，服务和教育的成本较高。

此外，根据 Ponemon 研究所 2011 年的年度调查美国公司数据丢失成本，在 2010 年每损失数据的平均成本是$214，比 2009 年上升 5%。根据这项调查，通信部门为客户记录承担$380 最高损失，其次是金融服务$353，接下来是医疗保健$345，媒体$131，教育$121，公共部门$81。

安全公司赛门铁克赞助 Ponemon 研究所开发的数据泄露风险计算器，可以用来计算在未来 12 个月数据破坏的可能性以及计算每次破坏和每记录丢失引发的平均成本和费用。

Ponemon 实验室估算直接损失，也可用于估算由 OSF DataLossDB 收集的数据泄露事故的直接损失。通过 2009 直接损失数据$60.00/记录，记录数与每一个事件报告相乘，以获得金钱上的损失估算。假设违背条款的一方将承担直接损失。然而并非总是如此，例如：除非信用卡号错误，将由银行或者发行单位承受直接损失。此外，估算费用不包括间接成本（如时间，精力和其他组织资源略去），以及机会成本（如因声誉受损导致失去商业机会产生的成本）。

另一种可能的方式是如果该公司将为数据丢失承担赔偿责任，那么作出消减潜在损失的风险管理决策是一定的。通过使用美国债务判例法中法律责任的定义，给出损失的概率（P），损失金额（L），再有就是有足够预防措施或承担（B）公司的成本的责任，

$$B < P \times L$$

通过应用该公式以来自美国联邦贸易委员会（FTC）2003 年的数据为例，遭受身份欺诈的人金额损失概率为 4.6%乘以通过因子分解受害人损失的数量，考虑到追回损失的时间来计算人员 3 亿小时所花费的支出金额以每小时$5.25/人工工资计算再加$50 亿支出。

$$L=（花费的时间\times从丢失开始的恢复\times每小时工资+实际开支）/受害人数量$$

用这个公式来计算由于身份造假事件导致的损失金额，根据 2003 年联邦贸

易委员会的数据，每个客户/受害人的损失大约是 655 美元，并征收该公司为每个客户/受害人在每次事故中所负担的 30.11 美元。

然后决定是否有可能来保护客户每年每位客户 30.11 美元损失的风险管理决策。如果可以，那么公司就存在需要承担责任的赔偿风险。这种计算对于确定数据丢失事件潜在赔偿责任风险的情况下是有用的，例如通过将美国联邦贸易委员会 2007 年的数字到 TJX 公司事件中它最初宣布的 4570 万客户机密信息的暴露，被曝光所涉及到的受害者可能被计算为

事件暴露损失 = 该事件导致受害者暴露的人数×每个受害者的损失

对于使用 TJX 公司数据或受影响的受害人数这个公式，并通过使用联邦贸易委员会施加于每个受害者的损失数据，表示潜在损失事件的成本是 300 亿美元。把这一事件发生的概率作为计算因子，那么它有可能确定多少钱应该花在保安措施。以 TJX 公司事件为例，假设千分之一机会出现的情况下 TJX 公司 3000 万美元的安全项目将是合理的。

数据泄露计算工具

赛门铁克根据 Ponemon Institute 在数据调查，提供了一个用于估算组织、整个行业在经历一次数据泄露后所产生的成本的计算器：

https://databreachcalculator.com/

估算漏洞攻击的概率

估算一个特定的 Web 应用程序漏洞的攻击的概率，大家可以参考从 Web 黑客事件数据库（WHID）数据的报告。WHID 是一个 Web 应用安全联盟（WASC）项目，提供从公共来源收集 Web 应用程序的安全事故统计分析信息。在 2010 年的 WHID222 类事件中，注意到，其中 33%的目的是为了占领网站（例如：使用拒绝服务），15%的目的是破坏网站，13%是为了窃取信息。其中攻击的总体类型是试图利用应用程序的漏洞，如 21％是通过 SQL 注入。

通过使用事件报道和分析 2010 年 WHID 数据，攻击旨在通过利用一个 SQL 注入漏洞来窃取信息的总概率是 13％×21％=2.7％。由于 SQL 注入也有报道用于篡改，这应该被视为粗略的估计。

2010 年 12 月至 2011 年 5 月由安全公司 Imperva 为期半年恶意网站的攻击流量的另一项调查发现，在确定 23%的攻击是 SQL 注入后，跨站脚本成为第三个最普遍的攻击，第二个最流行的是最为普遍的目录遍历攻击，他们分别占到所有攻击的 37%和 36%。

估算漏洞攻击对业务的影响

通过比较 WHID 和 Imperva 的 Web 攻击的调查，21～23％的攻击利用 SQL 注入漏洞数量级似乎是一个可以接受的概算。假如金融机构因为安全事件导致的数据丢失为$355/记录（Ponemon 研究所 2010 年的数据），对于一个公司的网站，这样的事件在 2010 年利用了一个 SQL 注入漏洞的概率为 2.7％（WHID2010 年数据），如网上银行的 100 万记录的数据丢失了导致的赔偿责任达$9585000。有了这个数字金融组织 2010 年防止数据丢失的风险特别针对 SQL 注入攻击应用安全措施的 900 万美元预算花费将是合理的。

假如你会花很多的费用在安全措施中，这些安全措施可以阻止 SQL 注入攻击，包括获取安全软件开发技术、文档、标准、流程以及人才的招聘和安全编码教育特别是对 Web 开发人员。通常这种美元的数字应该被认为是一个可以承担的最大值，例如：用户数据的总损失。

要注意的是注入漏洞是在OWASP（2013年A1注入）认为特别重要的有针对性的漏洞攻击，最关键的是利用应用安全风险。OWASP数据注入的风险包括SQL注入漏洞，正如其严重是由于“可能导致数据丢失或数据破坏、缺乏可审计性或是拒绝服务。注入漏洞有时甚至能导致主机完全被接管。” 我们计算一个中等规模的金融服务公司（100万注册网上银行的用户）假设数据资产的价值可以通过威胁代理被盗造成的公司有形资产损害导致赔偿责任造成的商业影响。

从历史看，SQL注入攻击在美国一直有很高的影响，已经出现的犯罪和被起诉的规模最大的数据泄露事件也与此有关。2009年8月美国起诉阿尔伯特·冈萨雷斯（2009年5月在马萨诸塞州的TJX公司违约事件也被起诉）及另外两名俄罗斯黑客在2007年8月利用SQL注入攻击闯入7—Eleven便利店网络导致信用卡资料被盗取的案件。据称，同一种攻击也在2007年11月用来渗透汉纳福特兄弟公司，导致420万借记卡和信用卡号码被盗，并在2007年12月从Heartland支付系统窃取1.3

亿信用卡号码。2010年，阿尔伯特·冈萨雷斯被判有罪并在联邦监狱服刑20年，而Heartland由于安全漏洞支付了1.4亿美元的罚款和清算。

总结

我们可以看到有很多不同的方法来确定信息的价值，而且其中的一些是纯粹根据有关数据泄露的成本。但总体而言，参考文献表明，通常个人的数据纪录可以在 500 元至 2,000 元范围内进行估价。

附录 B：OWASP 手册及项目快速参考

本快速参考对应典型CISO的功能和信息安全领域到OWASPCISO指南及其相关OWASP项目到不同部门

表2 对应到OWASP指南及其他项目的CISO功能

CISO 功能	安全域	OWASP CISO 指南	OWASP 项目
为应用安全开发和实施政策、标准和指引	标准与政策	I-3“信息安全标准，政策及合规性”	● 开发指南 - 政策框架 ● CLASP - 确定全局安全策略 ● SAMM - 政策与合规性 ● 代码审查指南 - 代码评价与合规性
开发，实施和管理应用安全治理	治理	III-3“应用安全治理，风险及合规性”	● SAMM - 治理 ● ASVS - 如何写工作需求
开发和实施软件的安全开发和安全测试流程	安全工程过程	III-4 “针对软件安全活动和 S-SDLC 过程” III-10“如何为您的组织选择合适的 OWASP 项目和工具”	● 开发指南 ● 代码审查指南 ● 安全编码实践 ● 测试指南 ● 全面的轻量级应用安全程序（CLASP）简介 ● CLASP 概念 ● 软件保证成熟度模型（SAMM） ● 测试指南 - 工具 ● 项目应用安全验证标准项目（ASVS）
开发，阐明和实施应用风险管理策略	风险策略	I-4“风险管理” II “管理应用安全风险准则” III-4“安全战略”	● SAMM - 战略与度量 ● 应用威胁建模 - 风险缓解策略

定义行政管理，业务管理人员以及内部审计和法律顾问工作有关应用的安全要求，可以进行验证和审核	审计与合规性	I-3“获取应用安全要求” III-3“解决 CISO 的应用安全功能”	● 应用安全验证标准 ● CLASP - 捕获安全要求 ● SAMM - 安全需求 ● 测试指南 - 安全要求测试推导 ● OWASP 聚宝盆 ● 安全软件合同附件
度量和监控组织内的应用资产安全和风险	风险度量与监控	IV“管理风险和应用安全投资度量”	● CLASP - 定义和监控指标 ● SAMM - 战略与度量 ● 应用安全度量的类型
界定，识别和评估关键应用资产内在的安全性，评估威胁，脆弱性，业务影响及对策建议/纠正措施	风险分析与管理	I-4“风险管理” II “管理应用安全风险准则”	● Web 应用程序的风险 Top 10 ● 移动应用风险 Top 10 ● 云计算风险 Top 10 ● ASVS - NIST 的风险管理验证活动实施 ● 风险评级方法 ● 威胁风险建模 ● 应用威胁建模
评估采购新的应用流程，服务，技术和安全工具	采购	III-4“第三方组件/服务采购之前评估风险”	● 项目安全软件合同附件 ● ASVS - 合同的需求验证
监督培训开发、操作和信息安全团队的应用安全	安全培训	III-5 “人员，流程和技术”	● CLASP - 学会宣传方案 ● 教育项目 ● APPSEC 培训视频 ● 视频会议 ● 应用安全常见问题

			● CLASP - 学会安全意识计划
制定，阐明和实施连续性规划/灾难恢复	业务连续性/灾难恢复	III-3“解决 CISO 的应用安全功能”	● 云业务连续性和弹性
调查和分析疑似和实际的应用安全事故，并提出纠正措施建议	漏洞管理和事件响应	I-4“应对发生安全事故后业务问题”	● SAMM 漏洞管理 ● CLASP - 管理安全问题披露过程 ● .NET 的事件响应指南

指南

- 开发手册

https://www.owasp.org/index.php/Category:OWASP_Guide_Project

  - 策略框架

    https://www.owasp.org/index.php/Policy_Frameworks

- 代码评审指南

https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project

- 标准手册

  - 应用安全验证标准(ASVS)

    https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

  - NIST的风险管理验证活动的实施

    https://www.owasp.org/index.php/How_to_bootstrap_the_NIST_risk_management_framework_with_verification_activities

  - 同要求的验证

    https://www.owasp.org/index.php/How_to_specify_verification_requirements_in_contracts

- 测试手册

https://www.owasp.org/index.php/OWASP_Testing_Project

  - 代码审计和合规性

    https://www.owasp.org/index.php/Code_Reviews_and_Compliance

  - 安全需求测试推导

https://www.owasp.org/index.php/Testing_Guide_Introduction#Security_Requirements_Test_Derivation

- 工具

https://www.owasp.org/index.php/Appendix_A:_Testing_Tools

其他项目

- 应用安全FAQs

https://www.owasp.org/index.php/OWASP_Application_Security_FAQ

- 应用威胁模型

https://www.owasp.org/index.php/Application_Threat_Modeling

  - 消减策略

    https://www.owasp.org/index.php/Application_Threat_Modeling#Mitigation_Strategies

- AppSec 培训视频

https://www.owasp.org/index.php/OWASP_Appsec_Tutorial_Series

- CLASP
  - 采集安全需求

    https://www.owasp.org/index.php/Category:BP3_Capture_security_requirements
  - 概念

    https://www.owasp.org/index.php/CLASP_Concepts
  - 定义和监视度量标准

    https://www.owasp.org/index.php/Category:BP6_Define_and_monitor_metrics
  - 识别全球安全政策

    https://www.owasp.org/index.php/Identify_global_security_policy
  - OWASP学会研究所宣传计划

    https://www.owasp.org/index.php/Category:BP1_Institute_awareness_programs
  - 介绍

    https://buildsecurityin.us-cert.gov/articles/best-practices/requirementsengineering/introduction-to-the-clasp-process

- 管理安全问题泄露过程

  https://www.owasp.org/index.php/Manage_security_issue_disclosure_process

- 云的业务连续性和弹性

https://www.owasp.org/index.php/Cloud-10_Business_Continuity_and_Resiliency

- 视频研讨会

https://www.owasp.org/index.php/Category:OWASP_Video

- 聚宝盆（*一个纸牌游戏形式的机制，以协助软件开发团队找出敏捷，传统的和正式的开发流程的安全要求。它是语言，平台和技术无关。*）

https://www.owasp.org/index.php/OWASP_Cornucopia

- 教育项目

https://www.owasp.org/index.php/Category:OWASP_Education_Project

- .NET事件响应

https://www.owasp.org/index.php/.NET_Incident_Response

- 风险评级方法

https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

- SAMM

http://www.opensamm.org/

  - 治理

    https://www.owasp.org/index.php/SAMM_-_Governance

  - 政策 & 合规性

    https://www.owasp.org/index.php/SAMM_-_Policy_&_Compliance_-_1

  - 安全需求

    https://www.owasp.org/index.php/SAMM_-_Security_Requirements_-_1

  - 战略 & 度量

    https://www.owasp.org/index.php/SAMM_-_Strategy_&_Metrics_-_1

  - 漏洞管理

    https://www.owasp.org/index.php/SAMM_-_Vulnerability_Management_-_1

- 安全编码实践

https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide

- 安全软件合约附件

https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex

- 威胁风险建模

https://www.owasp.org/index.php/Threat_Risk_Modeling

- Top 10云风险

https://www.owasp.org/index.php/OWASP_Cloud_%E2%80%90_10/Initial_Pre-Alpha_List_of_OWASP_Cloud_Top_10_Security_Risks

- Top 10 移动应用风险

https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks

- Top 10 Web 应用风险

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Projec

- 应用程序安全性指标的类型

https://www.owasp.org/index.php/Types_of_application_security_metrics

（附录部分翻译 樊山）