# 数据安全的商业论证

1.0 版

发布日期：2009 年 1 月 26 日

## 作者备注

本报告内容的开发与任何赞助商无关。本报告基于最初在 Securosis 博客上发布的资料，已经过 SANS 的改进、审校和专业编辑。

本报告由 McAfee Inc. 授权并与 SANS Institute 合作发布。

特别感谢 Chris Pepper 在编辑和内容方面给予的支持。

## 迈克菲公司授权发布

McAfee, Inc. 总部位于美国加利福尼亚州的圣克拉拉，是全球最大的专注于安全技术的公司。迈克菲始终致力于应对全球最严峻的安全挑战。迈克菲提供经实践验证的前瞻性解决方案和服务，保护全球的系统和网络，使用户能够更安全地联网并在 Web 上浏览及购物。迈克菲凭借屡获殊荣的研究团队，为家庭用户、企业、公共部门以及服务提供商提供创新产品和强大保护，使他们能够遵从法规、保护数据、防范破坏、发现漏洞以及不断监控安全问题和提高安全性。

http://www.mcafee.com/cn

## 版权

# 目录

# 简介

## 安全观念如何影响投资

在信息安全领域，我们面临着两大主要威胁：“喧闹”型威胁直接影响着我们开展业务的能力；“静默”型威胁会导致真正的破坏，但不一定会妨碍人们完成工作。病毒、蠕虫和垃圾邮件等“喧闹”型威胁会攻击网络和系统，无疑也会影响生产力和业务运作。由于存在极为明显（往往也极为令人烦恼）的攻击，因而易于论证投资的合理性，以遏制其影响。如果 CFO 看到自己的收件箱中有数以百计的垃圾邮件，那么他很可能会投资购买一个反垃圾邮件解决方案。

但数据窃取之类的“静默”型威胁可能潜伏了数年都未被检测到。当此类威胁最终被发现时，您可能无法计算这样的泄露已经导致了多少实际损失。如果无法直接证明相应的利润下滑或资产损失，则很难说服 CEO 签署一项数十万美元的投资。在很多情况下，例如信用卡被窃时，遭受损失的往往是其他人。因而，针对“静默”型威胁的安全投资往往是在法规或合同义务的要求下被迫实施的，而非出于自愿。威胁观念的缺乏影响着我们对数据安全的重视程度，进而影响着我们应对数据安全问题的能力。

## 具有竞争力的优先级：基础设施与资产

纵观安全市场，我们可以清楚地看到，针对“喧闹”型威胁提供保护的产品所占的资金份额远远高于针对“静默”型威胁的产品。如今的安全支出主要关注“边界”- 假定存在一个边界，将企业内部的用户和系统与所有其他人分离开来。并不是我们在边界安全方面失败了，或者投资不合理，而是系统和数据的使用发生了变化。我们使太多的信息可通过普通的 Web 浏览器访问，同时还增加了远程访问，并且更多地依靠分布式服务。在并行发展的过程中，我们所面临的风险发生了变化，而攻击者也意识到攻击我们的数据更容易也更有利可图。缺陷就在于我们的安全资源分布。从某种意义上讲，我们是自己的成功的牺牲品 - 由于企业已经很好地理解、广泛地实施了简单保护（如防火墙），因而这场战役已升级成更微妙、更棘手的问题。

这使我们陷入了一种悖论中。边界安全威胁仍然存在，而对信息资产的新型威胁需要截然不同的安全控制。我们常常陷入这样的预算循环：即便现有的安全机制不是应对当前问题的最有效方法，我们仍在持续更新该机制。获得更新维护协议或升级的许可比购买新产品容易得多。在管理过去的威胁时，我们也投入了大量的时间、培训和精力。我们能更好地理解风险、掌控成本、证明合理性。诚实地说，依靠已经掌握的知识总是比依靠需要学习的新知识更容易。

过去的威胁还有着永不消退的趋势，即便在今天，我们仍然能够看到十年前的病毒和蠕虫在 Internet 上蔓延。因而，我们不能只是抛弃旧基础设施来关注新威胁，但我们确实需要认识到，旧基础设施并非为应对新挑战而设计，我们的支出计算也往往陈旧过时。只有在遭受重大事件（通常是公共事件）之后或者在行业、政府的强制要求下，数据“静默”型威胁才能获得同等的投资。因而，我们为保护网络和系统所分配的支出远远超过为保护为我们的业务提供动力的信息资产的支出。“喧闹”型威胁曾经是我们最大的问题，但现在我们需要转移注意力。

## 构建商业论证

我们需要承认，威胁已经发生了变化，从“喧闹”型转变为“静默”型，从企业的边缘转向中心。我们还需要了解，攻击者的动机也已发生了变化 - 他们的目标已经不是破坏 Web 站点，而是欺诈和数据窃取。拒绝服务攻击、蠕虫、病毒和垃圾邮件仍然是难题，但这些“喧闹”型威胁作为数据窃取媒介的意义比作为最终目标更为重要。这不仅会导致生产力降低或些许尴尬，而且会给业务运作带来实实在在的风险。因此，问题就转变为：如何评估风险、调整投资，以关注业务的主要威胁？

有很多建议方法都展现出了为安全性投资、将数据安全看作一种投资所带来的获益，但在尝试论证在特定领域投资的合理性时，这些方法大多效果不佳。某些模型会尝试测量无法准确测量的方面，但往往会因其繁琐的过程而失败。还有一些方法仅依靠定性的推理，导致了极不准确的结果。大多数模型都包含成熟的经济规则的不合理变体，这些规则的设计目的是计量效率或投资回报率。对于安全来说，这是一种既不产生收入也不会带来完全可计量的结果的投资，必然会失败。

在这份报告中，我们将在构建合理性论证模型时关注数据安全（也称为以信息为中心的安全）的业务方面，帮助您确定在何处投资和投资多少来保护您的信息资产。首先，我们将分析一些常用方法失败的原因，讨论其弱点，强调应注意避免的一些常见陷阱。接下来讨论如何测量信息的价值，评估泄露可能带来的损失，计量导致这种损失的相关风险。以此为依据，我们将构建我们推荐的模型，结合不同的评估和合理性论证技术，论证它能给企业带来的额外价值。没有任何一种模型能反映所有企业的所有方面，我们希望您选择最适合您的模型。

不得不说，出于上面提到的原因，我们认为不可能完全依靠定量论证，但我们将为您介绍如何结合定量和定性因素来制定明智的风险管理决策。除了当作例子之外，我们不会讨论具体的技术，而是关注您在与管理层探讨时可能用到的业务方面。同样，这不是一种论证任何安全支出的合理性的通用模型，我们主要关注信息估价和数据安全。下文中所有对于信息估价、风险和损失评估以及正面获益（如降低 TCO 或审计成本等）的观察都基于这种以数据为中心的分析。我们的目标是为您提供必要的工具，评估您的环境，确定您面临的风险是否能论证安全支出的合理性。

# 数据丢失模型

## 理解数据的价值

安全是一种风险管理工具，其用途在于使企业能够以安全的方式承担他们所能够承担的最大风险量。按照定义，风险管理的主旨是限制损失或损失的可能性。但如果不能掌控您可能会失去的价值，就不可能理解损失。在这一节中，我们将深入探索信息的价值，在此过程中说明为什么不能总是指定具体的货币价值，但可以把握它对于企业的重要意义。与此同时，我们还将说明为什么依靠全面量化信息价值方法的模型注定会失败。

首先介绍一种量化和/或限定数据价值的方法，然后展示安全如何保护价值，这并不容易，因为在不同的业务环境中，价值会发生变化。我们可以根据卖点计算信息的价值，例如作为特定业务功能的支持因素、作为市场中的竞争优势或多种因素的组合。为了使我们的讨论明确化，我们将信息定义为有价值的数据，这也是我们倾向于使用术语“以信息为中心的安全”（而非“数据安全”）的原因之一。

但是，首先我们要强调一下常见模型的失败之处，说明为什么需要新方法。随后我们将介绍一种模型，该模型在可能时量化信息的价值、限定其他重要因素，并结合这两方面来评估价值。我们将提供具体示例，展示您以后可在企业中加以利用和细化的方法，以便更好地确定要为保护数据投入多少资金。此类投资要求您对要保护的资产具有深入的了解。

## 为什么数据安全无 ROI

第一个创建模型来准确计算信息的货币价值的人应获得诺贝尔奖。我们不能忽视数据的价值，但也需要接受一点：我们通常无法为其指定准确的货币价值。这就带来了信息安全领域中最令人烦恼的业务问题之一。安全项目需要进行与其他 IT 或业务项目相同的分析与论证，但其基本功能在于控制损失，而由于我们不了解我们所失去的东西的价值（这样的价值总在变化），所以也就不能准确预测损失。这并不是一种全新的思维方式，但其过程本身极为困难。使问题更加复杂的是，传统的投资和支出论证模型并不适用。用于计算的统计数据和度量指标通常不可用或不可靠，计算将收入和数据丢失视为对立的值。让我们通过一些模型来说明：

**投资回报率 (ROI)：**请复述下面这句话：安全支出无 ROI。其他任何说法都是错误的。具体原因如下：在将 ROI 应用于数据安全时，您要尝试量化损失，随后将损失代替收入。除了总是生成负面结果之外，还有几个原因使该模型从根本上不适于处理安全支出。第一个原因是安全防范不会带来回报或创造收入，因而从定义上来说，它们无法用于计算收入。由于代替了无法合理量化为“回报”的潜在损失而不是可量化的收益，因而该等式被误用了。此外，灾难恢复、诉讼费用和法规成本的预测可以达到一定的准确程度，但未来业务损失的货币价值则无法准确指定。ROI 是一种公认、常用的财务等式，但它并未考虑影响收入的许多相关变量，也未考虑多个事件泄露的非线性成本。这样的计算对于受控的学术问题来说是有效的，但在因数据泄露而导致的损失方面则完全是无用的输入、无用的输出。

**内部回报率：**某些企业使用内部回报率计算来评估支出，但这不仅会出现以资本回报代替损失的错误，还会导致尝试检查安全投资相对于其他形式的投资的效率这样的问题。由于信息的价值未完全量化，与不同风险度相关的损失不同，因而等式的最佳结果也只不过是大体预测。从实践的角度来看，这就像是尝试使用净现值，完全无用。

另外几种模型更为有用，也更加适合数据安全。ROI 计算的替代方案之一就是**安全投资回报率 (ROSI)**。它本质上仍然是 ROI 计算，但使用风险暴露的货币价值代替回报，并乘以投资所避免的威胁的百分比。另外一种替代方案是**年度损失期望 (ALE)** 计算，将单独一次事件的预计损失与预期出现率相乘。这两者都是较现实的方法，但都需要理解成本和之前/之后的出现频率。我们无法为信息指定准确的货币价值，这一点也会妨碍上述两种方法。在数据安全方面，我们没有可准确度量事件频率和成本的工具。

让我们具体观察一下 ALE，解释一下它的含义：考虑与笔记本电脑失窃有关的成本。企业可跟踪过去一年中失窃的笔记本电脑的数量。他们甚至还能跟踪包含信用卡信息的失窃笔记本电脑的数量，这提供了比较准确的出现率。企业还知道，要管理泄露通知，每条记录的成本是 3 美元，平均每台包含信用卡信息的笔记本电脑包含 10000 条记录。利用 ALE，他们可以准确预测每年因包含信用卡信息的笔记本电脑失窃而带来的成本，并将其与加密成本相比较。

当然，他们无法度量名誉或业务损失的成本，对于某一次事件来说，这些成本可能是 0，但如果多次出现此类事件，则可能会因失去所有客户的信任而破产。他们也无法度量与笔记本电脑上的知识产权损失有关的成本，因为不存在对通知的法规要求，所以关于出现率和业务影响的统计数据也是不可用的。请牢记，我们选择了易于度量的场景，而不是数据库泄露或信息泄露，在这些情况下，如果不首先实施数据安全保护，我们甚至无法进行度量。

在实践中，ALE 这种综合风险模型会在您将预测与猜测相结合、忽略未知条件时变为一种无意义的等式。要预测出现率，预测已经避免了多大比例的威胁，需要使用不可用的信息。就像我们说过的那样，猜测加猜测就等于毫无根据的乱猜。它的某些方面或许是有用的，但不能单纯地依赖它。因而，我们将在整体评估中结合定量与定性因素。

对于与丢失和失窃信息有关的成本，还有一个因素值得一提：“静默”型安全威胁并非针对网络或用户，而是针对数据。泄露、数据窃取或欺诈并非总是显而易见，欺诈的直接风险很可能将由其他人承担。例如，一次入室行窃之后，所有者本应发现物品失窃，但尽管数据被窃，原始信息原封未动，数据所有者也可能始终都不知道窃贼已拿走了一份副本。此外，欺诈本身可能并非针对企业，比如窃取信用卡数据的目的就是从另一家贸易商处购买商品。除了出现率之外，相关的货币损失也只是预测值，即便您已经注意到了事件的出现。为了明确这一观点，下面给出三个实际例子：

- 众所周知，许多流行歌曲、唱片和电影在正式发布之前即可在点对点的文件共享站点中找到。从表面上看，音乐厂商可计算其内容的非法共享量、将其与商品的零售成本相乘并得出损失数量，这似乎是合理的。但其他研究表明，非法交换最频繁的内容往往也是合法销售时最畅销的内容。有讽刺意义的是，有些厂商在考虑到这种效果后故意将内容透露给文件共享网络，以提高相应产品的总体需求，“非法副本”构成了病毒式营销的一种形式。因而我们可以看到，同一种情况有两种截然不同的数学模型，且无法确定任何一种模型的有效性。
- 在数据泄露通知法规出现之前，受到与信用卡或个人信息有关的数据泄露攻击的企业无任何损失。具体来说，如果信用卡号码被窃，丢失数据的企业进行交易的能力不会受到任何阻碍。而持卡人和发行银行将承担财务损失。因此，使用价值量化模型执行风险计算的企业找不到投资保护这些信用卡的任何理由。数据泄露通知法规改变了这种情况，迫使企业受到同等损失，但这些法规成本也会不必要地影响数据的价值（但如下文中所介绍的那样，它们确实提供了更好的基准）。
- 心存不满的高级销售管理人员在离开企业时收集各种知识产权信息的现象并不罕见，无论是报价单还是客户名单。许多此类人员最终都效力于竞争对手，并利用这些数据为新雇主服务。他们可能将销售工作的重点直接放在原企业的客户身上，虽然这并不意味着所有那些客户都将更换厂商，但确实提高了风险也改变了竞争的环境。除非事后再度量，否则无法度量任何损失，即便在事后，这些损失也无法用于准确预测类似环境下的未来损失。

## 信息评估的复杂性

有价值的数据称为信息。信息的整体价值取决于其环境 - 它所应用的环境、它的使用频率、有多少人能通过它获得价值。因而，信息技术对于任何企业的价值都在于其存储、管理、提供、分析和保护数据以支持业务运营并提供所有这些二进制数据的能力。某些类型的数据有着固有的价值：信用卡号码、身份证号码、军事服务记录、信用卡交易记录对于正确的受众来说都是很有价值的，因为他们能支持信用核查、聘用核查、贷款和保险申请。信用卡号码可能值 1 美元，具有相关姓名和地址的身份证号码可能值 5 美元。其他类型的数据都有派生价值。客户浏览和购买历史用于在浏览会话过程中推广产品，由于对销售有着直接影响，因而它们非常有价值。源于这些数据的客户服务、客户满意度、促销手段、业务分析和竞争差异化优势都是有价值的。但如上所示，数据的最终价值更为复杂，由多种因素共同决定，企业内可访问数据和通过这些数据派生信息的人越多，这些数据就越有价值。

### 为什么说信息的价值总是在变化，无法完全度量。

企业信息不断在被检查、插入、报告、比较、更新或以其他方式使用。所收集到的数据很少用于一种具体的目的，而是由许多人和许多业务单元用户用来满足多种不同的需求。来自不同数据源的数据将被结合和比较，以得到价值和其他洞察，帮助人们完成工作。这些数据还可与合作伙伴和客户共享，进一步扩展应用和提升价值。数据每一天都在变化，随着时间的推移，客户记录日益陈旧，失去了原有的价值，而其他一些信息越来越重要，越来越有价值。新客户不断增加，新产品不断售出。资产负债表也随之发生了变化，出现了新的支出。增加了客户的浏览历史、销售数据和营销指标，并得出了额外的度量指标。数据总是在变化，因而其价值也在不断变化 - 无论是变好还是变坏。即便是相同的数据，在不同的环境中也有着不同的价值，例如，一个没有对应姓名的信用卡号码只不过是一个 16 位的数字。这使分析数据价值成为一个连续不断的过程，有着不断变化的目标。

在本文档的后续内容中，我们将展示我们的模型，该模型设计用于应对其他模型中已发现的不足之处。下一节，我们将讨论数据对于您的企业的价值，以及如何在一个统一的模型内平衡不同的因素。

# 信息估价模型

我们知道数据拥有价值，但我们无法赋予它明确或固定的价值。我们希望使用价值来证明在安全上的花费是合理的，但仅仅依靠纯粹的量化模型来论证投资的合理性是不可能的。我们可以根据经验进行推测，但这些仍然只是推测，如果我们假定它们是可靠的指标，我们很可能会做出危险的错误决策。与其把注意力集中在难以实现（或无法实现）的定量价值度量上，不如使用定性评估开始我们的商业论证框架。请记住，这仅仅因为我们不量化数据的价值，并不表示我们以后将不在此模型中使用其他可量化的标准。这只是因为您无法完全量化数据的价值，并不表示您就可以抛弃所有指标。

为了切合实际，我们选择一个数据类型，并为其指定一个任意值。为了简化说明，可以选择介于 1 到 3 之间的数值，或者“低”、“中”和“高”来代表数据的价值。对于我们的系统，我们将使用介于 1 到 5 之间的数值更精细地度量，1 表示最低价值，5 表示最高价值。

另外两个指标在我们的估价过程中帮助处理业务环境：使用频率和受众。数据使用得越频繁，其价值越高（一般而言）。受众可以是公司内的一些人，或者合作伙伴和客户以及内部员工。使用的人越多且使用频率越高，通常表明价值越高，同时也越容易暴露给风险。这些因素不仅对于了解信息的价值非常重要，而且对于了解与其相关的威胁和风险（以及我们对开支的论证）也很重要。这两项将不会用作主要的价值指标，但是将修改一个“固有”值，我们将在下面更详细地讨论。像前面一样，我们将为每个指标指定一个介于 1 到 5 之间的数值，并且我们建议您至少宽松地定义这些范围。最后，我们将分析使用这些数据的三类受众：员工、客户和合作伙伴；并派生出一个介于 1 到 5 之间的分数。

一些数据的值根据时间或环境的不同而改变，在这些情况下，我们建议您为不同的环境分别进行定义和评价。例如，产品发布前的产品信息比发布后的同一信息更敏感。

以大学的学生档案为例。这些档案的价值很高，所以我们指定其价值为 5。虽然我们认为该数据的价值为“高”，因为它在财务上会影响学生，但是其使用频率只是中等，因为这些档案主要在一个可预测的时间段（每学期的开始和结束时期）内被访问和更新。此数据的受众数量为 2，因为这些档案被各种学校员工（财务和注册办公室）和学生（客户）使用。用表格表示如下：

| 数据 | 价值 | 频率 | 受众 |
|---|---|---|---|
| 学生档案 | 5 | 2 | 2 |

## 估价示例

做为一种基础训练，我们来看一看一些常见的数据类型，探讨一下它们的使用方式，并评估其对企业的价值。其中一些明显对企业有较高价值，但是其他类型不是这样。使用频率和受众对每个公司都不同。在您开始派生价值之前，您需要与主管和业务部门经理们坐下来，首先找出您依赖哪些信息，再使用这些评估场景帮助对信息进行分级，然后完成该论证模型的其他部分。

### 信用卡号

存储信用卡数据对很多企业来说是非常必要的 - 这是解决争端的常见要求。大多数商家都在因特网上销售产品，信用卡数据要遵循 PCI DSS 要求。除了满足这个最主要的功能，客户支持和营销指标也从该数据派生价值。此信息供雇员和客户使用，但是不与合作伙伴共享。

| 数据 | 价值 | 频率 | 受众 |
|---|---|---|---|
| 信用卡号 | 4 | 2 | 3 |

### 医疗信息（财务方面）

个人身份信息是最常见的攻击目标和诈骗的关键因素，因为它通常包含财务或身份识别信息。对于医院之类的组织，这种信息是非常必要的，而且广泛应用于治疗。虽然其访问频率可能为中等（或较低，当病人未接受治疗时），但它会被病人、医院工作人员和第三方（比如临床医生和保险人员）使用。

| 数据 | 价值 | 频率 | 受众 |
|---|---|---|---|
| 医疗个人身份信息 | 5 | 3 | 4 |

### 知识产权

从专利到源代码，知识产权有多种形式，所以与这种数据类型相关的价值在各个公司之间各不相同。对于上市公司来说，这可能是与项目相关的信息或可用于内部交易的投资信息。对于使用该信息的员工来说，其价值可能为中等，但是在临近每季度末和在其他信息公布时期，当将其向更广泛的受众公开时，其价值可能为高。

| 数据 | 价值 | 频率 | 受众 |
|---|---|---|---|
| 财务知识产权（一般情况下） | 3 | 2 | 1 |
| 财务知识产权（信息公开时期） | 5 | 2 | 2 |

### 商业秘密

商业秘密是另一种要考虑的数据类型。受众仅限于公司内特定的少数人，使用频率低，而商业价值可能非常高。

| 数据 | 价值 | 频率 | 受众 |
|---|---|---|---|
| 商业秘密 | 5 | 1 | 1 |

**销售数据**

已完成交易的销售数据的价值在各个公司之间差别很大。定价、客户名单和联系信息，都在公司内和公司之间广泛使用。在竞争对手手里，此信息可能会对销售和利润带来严重威胁。

| 数据 | 价值 | 频率 | 受众 |
| --- | --- | --- | --- |
| 销售数据 | 2 | 5 | 4 |

**客户指标**

客户指标的价值在各个公司之间有着根本的区别。例如信用卡发行商可能评定此数据有中等价值，因为它被用于欺诈检测，以及出售给商家和销售者。该信息被员工和第三方购买者使用，并提供给客户以查看开支。

| 数据 | 价值 | 频率 | 受众 |
| --- | --- | --- | --- |
| 客户指标 | 4 | 2 | 3 |

您可以创建更多类别，甚至货币价值范围等级，只要您觉得那有助于给您企业中的每个数据类型指定相对值。但是我们想强调的是，这些是定性评估，而不是定量评估，它们在您的企业中是相对的，而不是绝对的。重要的是展示您的企业在使用多种形式的信息。每种信息类型用于不同的业务功能，并且对企业来说有其自己的价值，即使该价值不是以金钱衡量的。

接下来我们将检验数据面临的威胁，并派生度量来洞察这些风险。

# 评估风险

## 度量和理解信息的风险

如果数据安全是主要的利润来源，我们会将商业论证讨论从信息价值转移到对其潜在利润的评估上。但是，既然数据安全不是主要的利润来源，那么我们就不得不预防出现价值降低的可能，从而指导在实际运作中是否需要采取任何措施。我们所需做的是了解直接威胁数据价值的风险以及应对这些风险的安全防范措施。安全，在其许多形式中是我们用于管理数据风险的主要方法，因此，了解相关的信息风险和安全投资，从而降低风险，对于平衡工作是不可或缺的。在本节中，我们将就信息风险和威胁进行探讨，而在下一节中，我们将讨论数据丢失。当我们整合模型时，我们可以根据可能的基于价值的风险、损失和收益而勾勒出未来的数据安全投资方略，从而进行整体论证。

毫无疑问，我们的数据总是处于风险中，不管是恶意攻击还是业内人士的偶然失误或是用户操作错误，我们几乎每天都会遇到数据的泄露和丢失。从高校、政府、个人到大中小型企业，都在不断遭受公共数据和私有数据的丢失。虽然我们都直观地感受到数据安全是一个非常重要的问题，但对于定量处理实际的数据风险还是有一定的困难。可能的威胁数量和盗窃信息的方法令人震惊，但当我们定量处理风险时，却没有足够的信息来正确理解风险对我们所造成的影响。

## 结合定量和定性风险评估

我们还可以通过另一种方法来评估风险；对可以定量的风险进行定量评估，对无法定量的风险进行定性评估，并将定量评估和定性评估组合到一个统一框架中。尽管我们可以度量一些风险，如丢失笔记本电脑，但是有些风险是无法度量的，如由于新漏洞的出现造成 Web 应用程序数据库的泄露。如果仅限于能够准确度量的风险，我们将对很多真实存在的信息风险束手无策。定量评估是一个强大的工具，可帮助我们了解风险和影响决策，帮助验证总体模型的有效性。

对于我们的商业论证模型，我们致力于简化风险评估流程，仅提供了解数据安全投资所需的内容。由于不同的数据类型所含的价值不同，且每个类型都面临着不同的风险，因此将风险分析用于特定的信息类型比用于通用分析要有效得多。在最后一节中整合模型时，我们将向您展示如何将风险评估与价值评估结合使用，以及通用评估在什么情况下仍然有效。

首先，我们先列出潜在的风险类别，然后列出每个风险可能发生的比率或年度发生率，最后列出对于机密性、完整性以及可用性的严重程度评级。对于风险事件，如丢失笔记本电脑及其中的敏感信息，我们可以使用数字做出较为精确的预测。在下面的示例中，我们知道年度发生率 (ARO)，因此填入了数值。而对于不可预测的风险，我们仅将其分级为“低”和“高”。然后划分出每个类别中的当前评估（或测量）级别。对于定性评估，我们将使用范围 1-5，此方法比较主观，您可使用任意一个范围来帮助您提高对风险信息的理解。

注意，估价是基于风险的；我们将在下一节中对潜在的数据丢失度量进行说明。虽然它看上去并不是很直观，但却可以说明用于减少多个风险类别的潜在数据丢失和降低复杂性的安全控制。记住，我们所关注的是商业论证，而不是整体的风险管理系统。我们希望能够分离这些元素，否则每个论证项目都会变为为期 2 年的风险评估。

**风险评估：信用卡数据（示例）：**

| | | 影响 | | | |
|---|---|---|---|---|---|
| 风险 | 可能率/ARO | C | I | A | 总计 |
| 丢失笔记本电脑 | 43 | 4 | 1 | 3 | 51 |
| 数据库泄露 (Ext) | 2 | 5 | 3 | 2 | 12 |

这是一个简化的商业论证模型风险记分卡。总计一项并不是用于比较某个风险类别和另一个风险类别，而是用于得出将在商业论证中使用的评估总计值，以显示可能对评估投资的削减。由于不同企业的风险类别各不相同，因此我们在此处使用了最为常用的数据安全风险，且在第 6 节中，我们将讲述如何将其整合到整个模型中。

## 常见的数据安全风险

以下内容为主要的信息丢失类别。每次数据泄露都是由以下一个或多个事件造成的。此处所列内容并不全面，仅提供了常见的数据安全风险类别，以供您快速实现模型。除了每种威胁攻击方法外，我们还会通过逻辑组来说明每个特定类别的风险和可能使用的解决方案都存在类似性。要考虑的主要类别如下：

### 丢失介质

此类别指某些包含静态数据的介质的丢失或被盗。介质包括磁盘驱动器、磁带、USB/存储棒、笔记本电脑以及其他设备。大多数数据丢失都属于本类别。常用的安全防范措施有以下几种：介质加密、介质“过滤”，在某些情况下使用终端数据丢失保护 (Data Loss Prevention) 技术。

- **丢失磁盘/备份磁带：**丢失备份介质是造成信息丢失的最大原因之一。任何时候，丢失介质的可能性都不大，但是由于介质的使用期限很长，因此这一风险会一直存在，直至风险消除。安全措施：介质加密和磁盘“过滤”，这两种方法都可显著消除此类风险。
- **笔记本电脑丢失/被盗：**从丢失或被盗的笔记本电脑上恢复的数据可能面临数据丢失的巨大威胁。笔记本电脑的风险非常高。安全措施：完整的磁盘加密可提供高度的安全保障。仅仅是不在笔记本电脑上存储敏感数据并不能达到很好的保护效果，但如果配合使用终端验证，就可以提供中等程度的风险消除。
- **退役服务器/驱动器引起的信息泄露：**服务器和组件的销售会导致数据的大量泄露。安全措施：磁盘“过滤”（需要修改流程，以便使用“过滤”工具）对此类风险很有效。在数据生命周期早期加密介质也同样有效。
- **便携式存储设备（存储棒/闪存驱动器）丢失：**便携式存储设备体积较小，可以保存大量数据，易于使用也易于丢失。它是最可能造成数据丢失的途径之一。安全措施：为员工提供内置了加密装置的“智能”存储棒，可以有效消除此类风险。通过 DLP 终端技术将数据移入/移出介质可以提供有效的控制。
- **服务器/工作站被盗：**与丢失介质或笔记本电脑相比，服务器或工作站被盗的可能性不高。但是，如果物理安全性不高，就会增加偷窃成功的几率。通常，偷窃服务器或工作站的目的不是数据，而是为了销售设备，数据丢失只是随之产生的副产品。安全措施：通常，提高物理安全性是最有效的方法。另外，完整的磁盘加密也非常有效，但可能会影响性能。

### 意外泄露

此类别包括以某种形式意外公布数据并导致不必要的泄露。例如，将电子邮件发送给了不必要的收件人、将机密数据公布到了某些网站、Internet 传输不安全、缺少访问控制等。安全措施包括以下几种：电子邮件和 Web 安全平台、DLP 和访问控制系统。每种措施都非常有效，但仅针对某些特定类型的威胁。同时，也需要通过流程控制和工作流控制来捕捉人为错误。

- **通过电子邮件意外泄露数据（监听、地址错误、文档元数据未清除）**：错误地发送客户或知识产权列表的现象很常见，故意通过邮件发送公司机密占很高比例，但大多数出站电子邮件都经过了扫描或审核，可识别出此类错误。安全措施：电子邮件安全产品对于检测电子邮件流中的敏感数据比较有效，大多数都可保证与合作伙伴间通信的安全性。但几乎很少有工具能够发现数据被发送到了错误的地址。
- **由于意外泄露而造成的数据泄露**（在网站上公布信息、打开文件共享、无保护的 FTP 或将数据置于不安全的位置）：预防此类风险所面临的一个最大挑战是如何捕捉数据处理人员所犯的错误。这种意外的人为错误可以通过策略控制和流程控制来消除，而在某些类型的事件中可使用 DLP。
- **通过不安全的连接泄露数据**：所监听的通信或交易信息被认为是安全的，但可通过 Internet 进行路由。很多这类泄露都是由内部配置和意外情况造成的，而且员工可能并不知情。安全措施：大多数电子邮件和 Web 安全平台都可提供安全的信件桥接和路由功能，如果适当配置将非常有效。对流程进行更改，添加定期查看，以检查路由到的安全网络是否正确设置，这一方法也十分有效。
- **通过文件共享泄露数据**：文件共享程序可用于移动大量文件（可能是非法的）。由于这些程序是非法的，因此都采取秘密的方法安装和使用，这使得安全人员无法查看其配置，也无法确定是否在无意间共享了业务文件。此方法造成的数据丢失通常都是故意的。安全措施：不允许使用文件共享程序可阻止很多泄露的发生。如果 Web 安全平台中整合了强大的网络安全功能，它将能够非常有效地检测和组织这些文件共享产品。

## 外部攻击/泄露

本类别描述数据窃取实例，在这些实例中，公司系统和应用程序遭到恶意攻击，机密性和完整性都会受到影响。典型的攻击包括：盗用帐户/密码、SQL 注入、网站攻击、特洛伊木马程序、病毒、网络“监听”等。系统遭到攻击后可能会安装其他的恶意代码。虽然不是最为常见的形式，但此类别造成的数据泄露最具破坏性，也可能会引发欺诈行为。任何安全防范措施都有助于检测此类风险；但是，评估、渗透测试、数据加密和应用程序安全都是很常见的预防控制措施；同样，应用程序和数据库监控、WAF 和基于流的检测与检测控制也非常重要。

- **通过盗窃帐户（弱密码）进行数据窃取**：若恶意攻击者猜中密码，数据将被盗。安全措施：要求使用强密码。要求定期更改密码。在 X 次登录失败后，冻结帐户。某些访问控制系统可强制使用强密码，自动化密码策略的实施，并取得了很大的成功，且很多渗透测试工具也会识别弱密码帐户。
- **网络/系统泄露**：传统的以数据为目标的外部工具也会对企业数据造成威胁。例如，发生网络泄露后，在金融交易途径中安装“监听器”可收集信用卡号码。防范错误包括传统的边界安全控制和出站数据安全，如 DLP。
- **数据库泄露**：数据库是一种非常复杂的应用程序。“数据库泄露”一词可用于数据库服务器上很多不同类型的攻击。具体的攻击现象包括：滥用特权、误用功能、缓冲区溢出和 SQL 注入。通常，数据库攻击的目标是偷盗数据库中的信息。在数据库中注入任意代码以改变其原始功能，或将数据库用作平台来攻击其他应用程序，这些都是很常见的攻击方法，可使用相同的方法进行预防。安全措施：使用数据库应用程序监控功能来检测攻击和误用。数据库漏洞评估。DAM 可用于监控数据库的使用，在本质上是一种检测控制机制。DAM 检测数据库所进行的查询，比较每个查询与已知的威胁模式和业务最佳实践，并对可疑事件采取预防措施。漏洞评估是一种预防性方法，可从数据库的配置、安装和使用方面针对已知漏洞和安全弱点对数据库进行检测。
- **Web 应用程序泄露（逻辑缺陷，漏洞攻击）**：此类别包括对为特定用户提供数据的 Web 应用程序的攻击。主要的漏洞攻击形式包括：误用 Web 应用程序平台、更改浏览器的会话信息、缓冲区溢出和 Web 应用程序的 SQL 注入。漏洞评估和渗透测试可提供高度的安全性，预防由逻辑缺陷和不安全的编程语言所造成的数据泄露。其他措施还包括基础设施保护以及对 Web 应用程序代码的修改。
- **不安全终端引起的泄露**：一种有效的攻击方法是攻击内部系统/终端，然后使用它在本地解压缩数据并攻击其他系统。标准终端安全实践可解决这一风险。

## 恶意内部攻击

本类别描述数据窃取实例，在这些实例中，公司系统和应用程序遭到恶意内部攻击，机密性和完整性都会受到影响。内部攻击威胁非常不好控制，因为员工、承包商和其他内部人员都是受信任的，且当其进行恶意攻击时通常使用的都是授权操作，因此无法检测出来。没有向其授予访问权限的内部人员可通过标准数据安全控件（访问控制、加密）来进行控制。使用授予的访问权限进行的恶意活动可通过基于策略的数据安全工具进行管理，如 DLP 和 Database Activity Monitoring。

- **由便携式存储设备引起的数据泄露（U 盘、CD/DVD）：**恶意的内部攻击者可将敏感数据转移到便携式存储设备上，以进行不正当的使用。可通过终端 DLP 或便携式设备控件进行管理。
- **由个人电子邮件/Web 引起的数据泄露：**恶意内部人员可使用基于 Web 的电子邮件服务（如 Hotmail）、Web 存储服务或个人 FTP 站点发送企业数据以供日后收集。此风险可通过 Web 过滤和 DLP 进行限制。
- **由内部人员（员工、合作伙伴、承包商）引起的数据库泄露：**数据库的所有用户都有使用数据库的凭据，但在角色、组和特定用户凭据之间，用户通常也具有执行本不应执行的操作的权限。数据库管理员具有的权限凭据通常可以执行数据库中的所有操作，但实际上仅应授予其执行一小部分功能的权限。虽然此类威胁与本节中所述的其他威胁类似，但这些漏洞更接近于实际事务，也更加难以被检测到。漏洞评估和渗透测试工具可检测权限使用是否过度；活动监控和审核技术可检测权限是否被滥用。

# 潜在损失

## 了解潜在损失

起先我们故意将潜在损失与风险影响分离开来，尽管损失明显是风险事件的结果。因为这是一个商业论证模型，而不是一个风险管理模型，所以我们可以解释主要的潜在损失（它们是多种风险类型的结果）类型并简化我们的整体分析。我们将着重强调与数据安全相关的主要损失类别，并使用我们的风险评估将它们划分为定量和定性类别。这些损失类别可以直接与风险评估相关联，并且有时可能对完成该训练很有意义，但是在我们完成我们的商业论证时，您将会看到为什么它通常是不必要的。

如果数据在一次安全泄露中被盗了，您会损失 100 万美元，还是 1 美元？您会注意到这些损失吗？在“数据丢失模型”中，我们介绍了一种方法来评估您公司拥有的数据的价值，以着重强调危险的数据。现在我们将提供一种技术来评估企业在数据丢失事件中的损失。我们看一些丢失类型及其影响。其中一些有硬性成本，可以比较精确地评估。另外一些更加模糊，所以指定货币价值没有意义。但是不要忘记，尽管我们可能无法完全量化这些损失，但是我们也决不能忽视它们，因为难以量化的成本可能具有很强的破坏性。

## 定量与定性损失

就像讨论“喧闹”型威胁一样，根据对生产力和效率有着明确影响的可量化威胁来论证安全开支的合理性要容易得多。对于数据安全，量化通常是极少的例外，实际损失通常结合了定量和定性元素。例如，您公司的一次数据泄露可能在发生很久以后才会引起注意。您仍然可以访问该数据，而且您可能未遭受到直接损失。但是如果该事件被公开了，您可能因此而面临法规和通知成本。被盗的客户名单和定价单、财务计划以及源代码都可能降低竞争优势并影响销售 - 或者也可能没有影响，这取决于盗窃者及被盗的内容。从您的公司盗窃的数据可能被用于欺诈，但是欺诈本身可以在其他地方进行。在身份盗窃中使用的客户信息会给您的客户带来很大麻烦，但是如果他们发现信息来源于您的企业，您可能面临处罚和法律责任。这占损失的很大一部分，尽管评估影响非常困难，但我们仍然必须解决潜在的损失，以论证防止或降低损失的开支的合理性。

有两种方法可用来结合定量和定性的潜在损失。在第一种方法中，浏览每种潜在损失类别，并为其指定一个估计的货币价值，或者用 1 到 5 之间的数值为其评级。这种方法比较快，但是不能帮助将潜在损失和您的承受能力联系起来。在第二种方法中，您创建如下表格，其中所有潜在损失按 1 到 5 的范围评级，表格中为（定量损失的）价值范围或描述损失级别的定性说明。此方法所需时间更长，因为您需要为每个损失类别确定五个测量点，但是允许您更容易地比较您的承受能力与潜在损失，并确定将潜在损失（或其可能性）降低到可接受水平的安全投资。

| 损失 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 通知成本（总成本，不是每个档案的成本） | $0-$1000 | $1001-$10000 | $10001-$100000 | $100001-$500000 | > $500000 |
| 信誉损害 | 没有由公开带来的负面影响 | 个别负面新闻报道，仅限本地/网络 | 持续的负面新闻，小于两周，仅限本地/网络，个别主要渠道报道。 | 持续不断的负面报道，大于两周，包括多个主要渠道。客户活动显著减少。 | 在主要渠道或全国范围内的持续负面新闻。客户活动极度减少。 |

## 潜在损失类别

这里是我们推荐的潜在损失评估类别，包括我们认为可量化的损失或只能定性分析的类别：

**可量化的潜在数据安全损失：**

- **通知成本**：CA 1386 及其他在发生数据泄露时通知客户的相关州法规。通知成本可以预先估计，包括联系客户以及任何信用监控服务，以识别欺诈活动。该成本与受影响的记录总数成线性关系。
- **合规成本**：大多数公司受其必须遵守的联邦法规或行业代码的限制。数据丢失和数据完整性问题使它们未能遵守法规。HIPAA、GLBA、SOX 及其他法规包括数据验证要求和不遵守这些要求的处罚。
- **调查和纠正成本**：调查数据是如何被影响的，以及纠正相关安全缺陷的关联成本，这些对企业来说都具有可以测量的成本。
- **合同/SLA**：有关服务质量或时效性的服务水平协议是很常见的，保密协议也一样。提供数据服务的企业依赖于数据的完整性、精确性和可用性；达不到任何一个方面都会违反 SLA 和/或使公司被罚款或损失利润。
- **信用**：数据丢失和 IT 系统受损都会被金融界视为投资风险信号。对利率和资金可用性造成的影响可能影响盈利能力。
- **未来的业务和信任**：数据丢失、不遵从法规或法规遵从处罚可能会妨碍您进行合同竞标，甚至会因为信用丧失而不能参与某些风险。这可能是永久的也可能是暂时的损失，但是其影响是可以感受到的。注意，未来的业务也是一种定性的损失 - 这里我们指确定的度量，比如被排除在业务市场外，与由于客户忠诚度/关注因素引起的潜在损失相对。
- **业务连续性**：拒绝服务攻击会影响客户服务和业务损失，因为数据或系统不可用。对于基于交易的业务，这通常是可测量的。

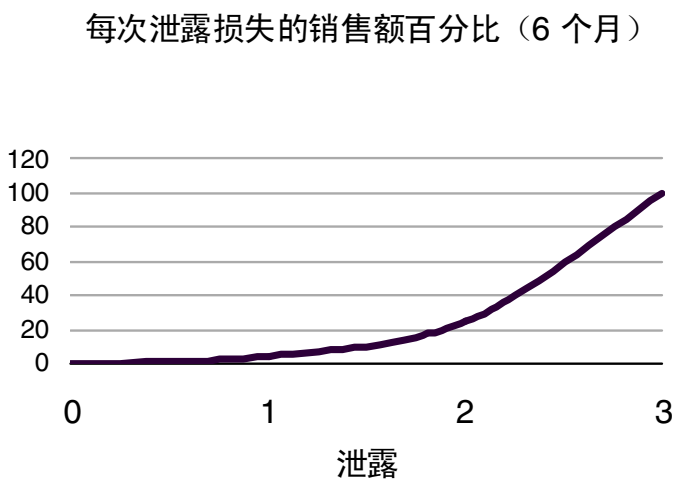
**可定性分析的潜在数据安全损失：**

- **信誉损害**：公司的信誉以多种方式影响其价值。新客户通常寻找他们了解和信任的企业。投资者喜欢购买值得信任并且高效运作的公司的股票。信誉风险对二者都会造成影响，但是一般无法将一个影响归因于单个事件，因为其他的事件、非风险因素以及一般的市场力量都会对客户行为产生影响。
- **客户忠诚度**：客户如何看待数据丢失会对客户和品牌忠诚度产生影响。如果数据丢失被认为是可预防的，并且带给客户的不便和财务损失很高，那么一些客户就会停止与该公司开展业务。
- **销售损失**：您的客户联系信息和定价单如果落到了您的竞争对手手中，就会为其有针对性的销售活动提供丰富的数据。他的所有成功都会让您付出代价。
- **竞争优势**：如果研究、源代码、流程或原料单被盗，则用于创造新的竞争产品的研发投资就会贬值；但是您仍然可以将该产品推向市场，所以损失的收益无法完全计算出来。
- **未来业务**：您无法精确预测损失的未来业务，除非将其限制在我们前面提到的市场/生态系统/合同之外。我们曾见到一个数据泄露事件就让一家公司破产的情形，而其他公司尽管也有严重的公共泄露，但是销量却增长了。

## 指数级损失增长

虽然单个事件带来的损失可能非常小，但是一系列事件将很可能以指数方式增加您的损失 - 尤其是在定性领域，比如名誉损害和未来业务损失。

尽管大多数调查都得出了结果，但是没有证据显示单个数据泄露和业务损失，甚至股票价格之间存在联系。例如，TJX 曾遭受过历史上最大的一次数据泄露，但是在整个事件期间其销售额仍稳步增长。很明显客户要么没有注意到，要么觉得发生该事件之后实施的安全控制措施会使在 TJX 购物更安全。但如果 TJX 在几个月内发生了一系列数据泄露事件，则该公司的业务在某一时刻将遭受实际的损失。




当为安全开支提供商业论证时，您不需要涉及损失的每一个方面。您甚至也不需要证明大多数数据价值都具有风险。相反，您需要知道有价值的数据具有风险，并分析安全和减少损失相对于这些投资的成本的潜在收益。实际的损害也许比较小，但潜在的损失却非常大。如果能够展示减少与数据盗窃相关的风险媒介也能够达到运营目标，那么论证将更有说服力。如果投资也涉及法规遵从控制，或者使业务流程更加高效，那么这项工作本身就可以收回投资。

# 其他积极优势

## 成本节省和其他积极优势

我们已经讨论了如何评估您公司所使用信息的价值以及数据失窃可能造成的损失。坏消息是安全开销只减少了部分威胁，但不能完全消除威胁。虽然我们希望我们的解决方案能够根除威胁，但实际情况往往非常复杂。好消息是安全开销通常可满足其他领域的需要。大多数安全产品会内置收集、分析和报告功能，当用于业务处理方面时，可作为现有应用程序和系统的补充。例如，安全投资可以立即给其他方面带来效益，如降低合规成本，改进系统管理，高效分析工作流，以及获得对数据使用方式和位置的更好的认识。其结果是通过自动化持续获得更好的效用并减少成本。我们将在分析中深入讨论这些问题，以及次要的优势如何创造附加价值。

### 减少合规/审计成本

法律规章要求监控特定的过程以实现策略遵从性，并要求进行后续验证来确保那些策略和控制措施符合遵从指南的要求。由于大多数安全产品都会检查业务流程以查找可疑的误用或安全违规，因此这与合规控制具有很大的相同部分。Gramm-Leach-Bliley Act (GLBA)、Sarbanes-Oxley (SOX) 和 Health Insurance Portability and Accountability Act (HIPPA) 中的某些规定可能要求安全性、过程控制或交易审计。数据安全工具及产品专注于解决安全和适当使用信息的问题，因此也可以构造策略来解决合规问题。

让我们看几种安全技术帮助实现合规性的方式：

- 通过向审计人员提供信息以快速验证控制措施的有效性和完整性，过滤、分析和报告可帮助减少审计成本；收集信息通常是审计中的很大一笔开销。这是数据安全工具减少审计成本的一个最有效的方法，而且能够显著节省成本。
- 访问控制帮助划分运营、管理和审计角色的职责。
- 电子邮件安全产品提供了 GLBA 要求的安全保障规则和借口防护 (Safeguards Rule and Pretexting)。
- 活动监控解决方案执行事务分析，与其他策略结合使用可以为期末调整 (SOX) 提供流程控制，以及解决 GLBA 要求的“安全保障”问题。
- 安全平台分离了数据收集、数据分析和策略实施角色，可以直接向不需要考虑安全性的适当的接收人发出警告。
- 收集的审计日志与自动化过滤和加密相结合，解决了常见的数据保留问题。
- DLP、DRM 和加密产品能够帮助符合 HIPAA 并帮助适当地使用学生档案 (FERPA)。
- DLP 工具使用内容发现识别敏感数据的位置，以减少手动发现/审计的时间，并向内部补救或外部审计人员提供报告。
- 这些工具可以缩小审计范围，识别哪些系统包含管制信息，排除不包含管制信息的系统。
- 审计技术提供了一个事务活动视图，并建立了有效和适当的控制措施。

## 更少的 TCO

数据安全产品收集各种信息和事件，这些信息和事件超越了安全性本身。它们提供了一个普通工具来收集、分析和报告与法规、行业和业务流程控制相关的事件；将大量的分析自动化，并与其他知识管理和响应系统集成。其结果是，除了主要的安全功能，它们还可以增强现有 IT 系统。安全和一般 IT 系统的总体拥有成本都减少了，两方面相辅相成，可能不需要额外的员工。让我们看几个案例：

- 系统和控件对财务数据的自动检查减少了内部审计人员的手动检查工作。
- 系统管理得益于对单调的信息服务检查的自动化，验证服务是否根据最佳实践进行配置，这可以减少破坏和系统宕机，从而减轻维护负担。
- 安全控件可以确保遵守业务流程和检测操作失败，在现有故障单系统中生成报警。
- DLP 工具使用内容发现，可以缩小必需的安全控制范围，识别涵盖的信息的位置，排除不要求相同安全级别的其他位置。

## 减少风险

您的评估过程的重点在于确定是否能够论证将一笔钱花在某个产品上或用于解决特定威胁的合理性。这个重点非常不错，但数据安全是一个企业级问题，所以应该从全局考虑。数据安全产品与一般的风险降低存在许多相同之处，类似于这些产品减少 TCO 并增强其他合规工作的方式。在汇编您的权衡列表时，将其他领域的风险或好处也考虑进去。

- 评定和渗透技术能够发现弱点并减少暴露；保持数据和应用程序安全可帮助保护网络和主机。
- IT 系统互联和共享数据。将威胁限制在一个业务流程区域中，这可以帮助改进连接区域中的可靠性和安全性。
- 发现功能可以帮助分析流程和了解风险暴露，定位数据并记录在企业中使用它的方式，确保遵从使用策略。

## 使用数据安全来设定其他投资的优先级

我们提供了一个模型来帮助您论证安全开支的合理性，但这并不是说我们的目标是扩大安全开支。我们的方法是注重实效的，如果您能够不使用其他安全产品来支持应用程序而达到同样的效果，我们完全支持。安全性大多以相同的方法来减少 TCO，一些产品和平台内置了安全性，因此可以避免其他的安全开支。我们承认数据安全选择通常是最后作出的，在为业务过程部署应用程序*之后*，并且在选择基础设施来支持业务应用程序之后。在评估平台时，内在的数据安全功能和与现有数据安全基础设施集成的简单性都应该是任何分析和概念证明过程的组成部分。Web 应用服务器、数据库服务器和各种企业应用程序平台都会经常评估功能以及对不同的开发和操作环境的支持，而安全往往是事后产生的想法。请切记，在购买（甚至部署）后再向应用程序或平台添加安全性可能是昂贵的，您在阅读本文和实际应用时可能已经意识到了。我们强烈建议在总体上保持数据安全，在评估用于数据处理的新应用程序时，要特别考虑本文列出的考虑因素，并注意产品的不足情况。在购买过程中做好长远打算可以节省资金，并避免以后遇到令人头疼的问题。

# 商业论证

## 构建商业论证

我们已经讨论了各种不同的商业论证元素，下面将这些元素放在一起形成一个完整的过程。根据项目的驱动因素，我们将使用以下两个选项之一：

- 基于投资的论证，用于评估特定的技术、流程更改或其他投资，具有模糊的保护目标。例如，“我们正在考虑投资 DLP”。
- 基于目标的论证，用于解决某个特定问题。例如，“我们需要保护我们的信用卡号码以符合 PCI。”注意，只有选择了某个技术、流程或其他投资之后才能使用基于目标的论证模型，但这并不意味着帮助您找到正确的作业工具，而是评估已经纳入考虑范围的工具。

由于基于目标的项目在范围上受到的限制比较多，因此我们将深入探讨基于投资的过程，然后向您介绍如何针对基于目标的项目对其进行修改。

我们在附录 A 中附带了一个数据安全商业论证工作表示例，随着我们对这个过程的讲述，参考该工作表可能对您有所帮助。

### 预评估

如果您希望评估多个数据安全选项，或者构建一个数据安全战略，我们建议您在继续进行进一步商业论证或评估之前进行数据估价、进行风险评估以及潜在损失评估。这将为您提供必要的信息，您可以在多个项目中利用这些信息，这些信息包括产品评估和规划数据安全战略，甚至可以协助您进行风险评估。

- 数据估价：由业务部门经理和其他管理人员使用，列出主要信息/数据类型并按照前面所述完成估价。然后根据敏感度按等级对其进行排列，以帮助确保任何数据安全投资符合企业优先级。
- 风险评估：从此处包含的数据安全风险类别开始，然后进行添加或删除以符合您自己的运作、法规以及协议要求。然后进行风险评估。由于某些风险类别不一定符合特定数据类型，因此您可以针对所有数据类型或其中某个子集进行风险评估，从而将其限制为广泛的类别（例如，PII 和知识产权）或者默认对暴露给该潜在风险的最敏感信息进行分析。我们建议针对 3-5 个最敏感的数据类型进行风险评估。
- 损失评估：从该报告中包含的潜在损失类别开始，根据需要进行调整以便与您自己的运作、法规或协议配置文件相匹配。与风险评估一样，您可以进行深入分析，也可以将损失评估局限于比较关键的数据类型、广泛的类别或暴露给每种潜在损失的最敏感数据。

## 步骤 1：定义产品/技术、流程或投资

列出特定产品、技术、流程更改或投资（例如，业务合作、服务或新的雇佣）以及简要描述，包括解决的业务问题（只有当论证针对的是技术人员时才使用技术描述）。

列出任何成本估算；所需的资金数额或全职等效时间。

| 投资 | 成本 | 说明 |
|---|---|---|
| | | |

## 步骤 2：将投资映射到所包含的数据类型和价值

详细介绍哪些数据类型可能会受到投资的保护，以及每种数据类型的价值、频率以及受众。应该对这些内容按等级进行排列，最有价值的数据位于最上面。除非您有意强调安全缺口，否则不需要列出投资不保护的数据类型。

该步骤是进一步继续之前的严格测试。如果投资不保护所需或所期望的数据类型，则该投资不是最佳匹配投资，因此应该放弃。工作表上包含的说明区域概述了潜在投资保护列出的数据类型的方式以及原因。

| 数据类型 | 价值 | 频率 | 受众 |
|---|---|---|---|
| | | | |
| | | | |

## 步骤 3：确定投资减少潜在风险的能力

如果进行潜在投资，则需要对所包含的数据类型进行风险评估，然后针对您的预期调整评估。根据您的目标，您可能需要对不同的数据类型进行风险评估，侧重于一种数据类型或进行更快但不太精确的常规分析。

| | | | 影响 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 风险 | 可能性/ARO | | C | | I | | A | | 总计 | | % Δ |
| | 之前 | 之后 | B | A | B | A | B | A | B | A | |
| | | | | | | | | | | | |

该部分说明潜在投资降低评估的风险的能力。说明区域概述了降低风险的方式以及原因，并且强调了最高风险或重要风险的减轻。

## 步骤 4：确定投资减少潜在损失的能力

如果进行投资，则需要对所包含的数据类型进行潜在损失评估，然后针对您的预期调整评估。根据您的目标，您可能需要对不同的数据类型进行风险评估，侧重于一种数据类型或进行不太精确但更快速的常规分析。

如果您已经进行了完整的潜在损失分析，则不用再查看整个表，只需列出偏移（变化）即可。

| 损失 | 1 | 2 | 3 | 4 | 5 | B | A |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |

该部分提供投资降低评估的损失的能力。在某些情况下，结果将是定量的资金数额；而在其他情况下，它将是定性的降低。工作表上的说明区域详细介绍了最相关的潜在损失降低，以及该产品提供这些功能的方式和原因。

## 步骤 5：详细介绍投资带来的其他优势

详细介绍数据安全投资所带来的其他可能优势，包括定量和定性的结果。

| 优势 | 说明 | 估计价值 ($) |
|---|---|---|
| | | |
| | | |
| | | |

## 步骤 6：总结商业论证

现在，您已经完成了工作表，并且拥有了什么是潜在投资、它保护什么数据、它如何降低风险、它如何降低潜在损失以及任何其他优势的概述。使用该信息进行详细汇总，并且当您绝对确信论证是针对技术管理人员时，仅使用技术语言。强烈建议您侧重于最重要的优势，而不是包括所有内容，这样您可以始终附加上完成的工作表，如果合适还可以对其进行更详细的分析。

下面是有效的商业论证的一些示例：

- 对 DLP 内容发现（静止数据扫描）进行投资将通过提供所有 PCI 数据位置的最新详细报告使我们的 PCI 相关审计成本降低 15%。这转换为 $xx/年审计。

- 去年我们丢失了 43 台笔记本电脑，其中 27 台包含敏感信息。笔记本电脑全驱动器加密对于所有移动工作者来说可以有效消除这个风险。由于 Y 工具还集成了我们的系统管理控制台并且确切地告诉我们哪些系统进行了加密，因此这会将未加密的笔记本电脑发生泄露的风险降低 90%。
- 我们的 SOX 审计人员需要我们在 2 个财政季度之内对财务应用程序的数据库管理员实施全面监控。我们估计这将为我们节省 X 美元（使用本机审计），但管理员将能够修改日志并且每个审计周期我们也将需要 Y 个工时来分析日志和创建报告。数据库活动监控花费为 %Y，这高于原始审计费用，但通过和日志关联并提供合规报告，它将 DBA 修改日志的风险降低了 Z%，将审计成本降低了 10% – 潜在净收益为 $ZZ，更高的安全性是一个辅助优势。
- 安装全部 DLP 套件将受保护数据被放置在 U 盘上的机会降低了 60%，将通过电子邮件将其发送到企业之外的机会降低了 80%，并且将员工将其上载到其个人 Web 邮件帐户的机会降低了 70%。

### 基于投资与基于目标的评估

在基于目标的评估中，您可以缩小评估范围，只调整已定义目标中受潜在投资影响的那些方面。例如，如果您的目标是保护数据库中的信用卡数据，则仅将分析限制于这一个数据类型以及与数据库中信用卡关联的那些潜在风险和损失。

在基于投资的评估中，您的范围可能更广泛，因为您要查找该产品的所有潜在数据安全优势，这可能会跨越多个数据类型、风险、损失类别以及其他优势。

## 结束语

数据安全花费论证是一项比较困难的挑战：无论是否花费、花费多少以及花费的地方，这都是非常难以解决的问题。数据安全保证了重要评估，但无法在 ROI 计算中捕获围绕信息安全的多方面问题。典型的优势计算不足以解决所涉及的复杂问题，并且对于诸如“我应该投资该产品吗？”之类的常见问题无法提供有意义的指导。如果您觉得您需要一个硬性的底线数字，请选择 Hitch-Hiker’s Guide to the Galaxy 的一个副本来获得答案。如果您想获得对可用于您的选择的有意义的评估，请遵循我们的模型。为了提供与您的企业相关的一些数据以及进行某些艰难抉择，您将不得不进行较深入的研究工作，本文所提供的框架将帮助您执行这个过程。

该报告的目标是帮助您分析为数据安全花费建立商业论证时的重要因素。**我们需要强调的是这并不是要发扬盲目花费**，而是提供一种在选择之间进行对比分析的方法。在更基本的级别上，我们的目标是就与 IT 花费有关的复杂问题提供实用建议。您的问题可能类似于“我是投资 X 技术还是投资 Y 技术来解决我的安全问题？”，或者“这是解决 ABC 合规问题的经济有效的方法吗？”为了帮助解决这些问题，我们需要采用另一种方式来看待该问题。无需从等式中巧妙地计算出底线货币成本，我们简单地将该问题归结为它的基本元素，然后在特定情形下评估这些因素。可以在最终结果中使用它本身，但我们建议将不同的解决方案相互比较，或者将一个选择集与另一个选择集相比较，因为这些结果可能会使您大吃一惊。

本指南旨在用作战略用途。尽管我们将该问题简单地归结为价值和风险的特定元素，以提供最佳的可能估计，但不要陷入特定技术或问题的具体细节。我们希望您使用该框架来更广泛地检查可用的选择。信息安全投资决策很少侧重于单个产品或问题，因此该工作表在设计上非常灵活，足以进行多因素分析。我们希望您将发现本指南适用于解决“喧闹”型问题的现有投资，有助于确定是继续那些投资还是重新投资其他领域。

最后一个建议是保留您的分析副本，必要时再次查看这些分析数据。您将发现其中一些比较是基于纯粹的合格数据或是您认为不稳定的因素。威胁、目标、数据价值以及您对风险的承受能力都会随时间而改变；而您总会找到更好的方法来量化这些因素。这就导致您的分析总是处于逐渐过时中。因此定期重新评估非常必要，可以确保您不断跟踪、重新验证目标以及在必要时调整您企业的期望。

# 数据安全商业论证工作表

## 步骤 1：定义产品/技术、流程或投资

列出特定产品、技术、流程更改或投资（例如，业务合作、服务或新的雇佣）以及简要描述，包括解决的业务问题（只有当论证针对的是技术人员时才使用技术描述）。

列出所有成本估算；所需的资金数额或全职等效时间。

| 投资 | 成本 | 说明 |
| --- | --- | --- |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## 步骤 2：将投资映射到所包含的数据类型和价值

详细介绍哪些数据类型可能会受到投资的保护，以及每种数据类型的价值、频率以及受众。应该对这些内容按等级进行排列，最有价值的数据位于最上面。除非您有意强调安全缺口，否则不需要列出投资不保护的数据类型。

| 数据类型 | 价值 | 频率 | 受众 | 等级 |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

| 说明 |
|---|
| |
| |
| |
| |
| |

## 步骤 3：确定投资减少潜在风险的能力

如果进行投资，则需要对所包含的数据类型进行风险评估，然后针对您的预期调整评估。根据目标，您可能需要对不同的数据类型进行风险评估、侧重于一种数据类型，或进行不太精确但更快速的常规分析。

| | | | 影响 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 风险 | 可能性/ARO | | C | | I | | A | | 总计 | | % Δ |
| | 之前 | 之后 | B | A | B | A | B | A | B | A | |
| 意外暴露 | | | | | | | | | | | |
| 电子邮件泄露 | | | | | | | | | | | |
| 不安全的连接 | | | | | | | | | | | |
| 文件共享泄露 | | | | | | | | | | | |
| 帐户泄露 | | | | | | | | | | | |
| 数据库泄露 | | | | | | | | | | | |
| 网络/系统泄露 | | | | | | | | | | | |
| 滥用特权 | | | | | | | | | | | |
| Web 应用程序泄露 | | | | | | | | | | | |
| 终端泄露 | | | | | | | | | | | |
| 磁盘/磁带丢失 | | | | | | | | | | | |
| 笔记本电脑丢失/被盗 | | | | | | | | | | | |
| 退役的介质 | | | | | | | | | | | |
| 便携式存储器丢失 | | | | | | | | | | | |
| 工作站/服务器被盗 | | | | | | | | | | | |
| 内部人员 - 便携式存储 | | | | | | | | | | | |
| 内部人员 - 电子邮件/Web | | | | | | | | | | | |
| 内部人员 - 数据库 | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

| 说明 |
| --- |
| |
| |
| |
| |
| |

## 步骤 4：确定投资减少潜在损失的能力

如果进行投资，则需要对所包含的数据类型进行潜在损失评估，然后针对您的预期调整评估。根据目标，您可能需要对不同的数据类型进行风险评估、侧重于一种数据类型，或进行不太精确但更快速的常规分析。

如果您已经进行了完整的潜在损失分析，则不用再查看整个表，只需列出偏移（变化）即可。

| 损失 | 1 | 2 | 3 | 4 | 5 | B | A |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 通知成本 | | | | | | | |
| 合规成本 | | | | | | | |
| 调查和修正成本 | | | | | | | |
| 合同/SLA | | | | | | | |
| 信用 | | | | | | | |
| 未来的业务和信任 | | | | | | | |
| 业务连续性 | | | | | | | |
| 信誉损害 | | | | | | | |
| 客户忠诚度 | | | | | | | |
| 销售损失 | | | | | | | |

| 损失 | 1 | 2 | 3 | 4 | 5 | B | A |
|---|---|---|---|---|---|---|---|
| 竞争优势 | | | | | | | |
| 未来业务 | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

| 说明 |
|---|
| |
| |
| |
| |
| |

## 步骤 5：详细介绍投资带来的其他优势

详细介绍数据安全投资所带来的其他可能优势，包括定量和定性的结果。

| 优势 | 说明 | 估计价值 ($) |
|---|---|---|
| 更低的合规成本 | | |
| 更低的审计成本 | | |
| 更少的 TCO | | |
| 其他风险降低 | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| 说明 |
|---|
| |
| |
| |
| |
| |

## 步骤 6：商业论证总结

总结您期望从潜在投资中获得的主要优势，包括受保护的信息、降低风险的能力、潜在损失减少以及其他积极优势。

# 关于

## 关于作者

**Rich Mogull**，创始人

Rich Mogull 在信息安全、物理安全以及风险管理方面拥有超过 17 年的丰富经验。在创立 Securosis 之前，Rich 在 Gartner 担任了 7 年首席安全分析师，为数千个客户提供建议，并撰写了数十份报告，是公认的 Gartner 顶级国际演讲者之一。此外，他在数据安全技术方面的工作也非常出色，他研究的问题范围广泛，从漏洞和威胁到风险管理框架，再到主要应用程序安全。Rich 是 TidBITS 的安全编辑、Dark Reading 的每月专栏作家，他还经常向很多刊物投稿，涉及范围从信息安全杂志到 Macworld。

**Adrian Lane**，高级安全战略家

Adrian Lane 作为高级安全战略家，有着 22 年的行业经验，他在 Securosis 团队担任了超过 10 年的 C 级执行专家。Lane 专门研究数据库架构和数据安全。作为供应商社区的成员，他有丰富的经验，包括曾经在 Ingres 和 Oracle 供职，是 CIO 角色中的 IT 客户，他还提出从面向业务的角度进行安全实现。在加入 Securosis 之前，Lane 曾经是数据库安全公司 IPLocks 的 CTO，在该公司负责产品和技术愿景、市场战略、PR 和安全宣传。Lane 还担任过 Touchpoint 的工程副总裁，在代理公司 CPMi 担任了三年 CIO，并且在安全和数字版权管理公司 Transactor/Brodia 担任了两年 CTO。Lane 拥有加州大学伯克利分校的计算机科学学位，毕业后他在斯坦福大学从事操作系统的工作。

## 关于 Securosis

Securosis, L.L.C. 是独立的研究和分析实践机构，注重思想领导性、客观和透明。我们的分析都是站在管理层的角度实施的，旨在提供最高价值的咨询服务。

我们主要提供四个领域的服务：

- 发布和演说：包括独立、客观的白皮书、网络广播以及亲自演示。
- 面向供应商的战略建议：包括市场和产品分析、战略、技术指导、产品评估以及合并和收购评估。
- 针对最终用户的战略建议：包括产品选择帮助、技术和架构战略、教育、安全管理评估以及风险评估。
- 投资者支持：技术尽职调查（包括产品和市场评估），以及与我们的研究合作伙伴合作进行的深入产品评估。

我们的客户众多，从秘密创业者到某些最知名的技术供应商和最终用户。客户包括大型金融机构、机构投资者、新运作的公司、中型企业以及主要安全供应商。

Securosis 已经与安全测试实验室建立了合作伙伴关系，旨在提供唯一的产品评估，其中包含深入的技术分析以及高级产品、架构和市场分析。

## 关于 SANS Institute

到目前为止，SANS 是全球最大、最受信赖的信息安全培训和认证机构。它还开发并维护了最大的与信息安全各方面相关的研究文档集合，并免费提供这些文档，同时它还运营着 Internet 早期警告系统 - Internet Storm Center。

您可免费访问大量宝贵的 SANS 资源。这些资源包括：非常流行的 Internet Storm Center、每周新闻摘要 (NewsBites)、每周漏洞摘要 (@RISK)、Flash 安全报警以及超过 1200 篇获奖的原创研究论文。