白皮书

将 IT 安全转变为有效的企业风险管理

将 IT 安全转变为有效的企业风险管理

综述

无处不在的安全数据目前尚不够切实和准确，因此无法指出在利用技术实现商业流程自动化时所可能导致的风险。无论是扩展地区性中枢还是整合被并购企业的信息技术（IT）部门，无论是选用一个新的网络运营商还是开设新的海外办事处，企业决策者都必须了解在利用技术改善企业业务流程时所面临的风险。

那种“我们会查出来的”的态度实在是太司空见惯了，虽然说这种态度是坦诚的，但遗憾的是，它并不能最有效地解决问题。IT 机构一般都不会毫无准备，而是会进行一些“猜测”并指望籍此在将来避免风险。困扰着多数企业的“我们真的不知道”现象的根源在于若干因素，包括:

- IT 机构人员短缺、工具不足
- 不能轻松地发现和整合目前所部署的多种不同信息系统所产生的大量数据
- 缺乏可将数据转变为有意义和可行性信息的、以企业为核心的风险管理应用

安全信息管理（SIM）的目的就是要消除这些欠缺之处，同时还要提供评估商业风险和技术漏洞时所需要的洞察力。目前主要用于收集和组织与安全事件相关的数据的SIM产品可被视作针对安全事件的电子卡目录系统。如果这就是它的全部功能，那么SIM产品就能极大地提高效率和意识，特别是对于那些需要操作入侵检测系统（IDS）和处理太多数据，而掌握太少实际知识的IT 人员更是如此。

遗憾的是，就能否找出与关键业务和应用系统直接相关的问题而言，有一些SIM产品存在着缺陷。某些SIM产品看不到企业资产的价值和非安全事件的数据，因此就不能明确揭示出在企业用来经营各自核心业务的“企业”系统中所存在的风险。

供应商所增加的功能可将基于 SIM 的安全监控提升到更高的水平：妥善管理与技术的日常使用相关的企业风险。

然而，这些安全管理系统的供应商正在增加新的功能，因此会很快将 SIM 提升到更高的水平：也就是将妥善管理与日常使用的、IT 生产运作中所部署的技术相关的企业风险。在 2003 年，SIM 产品日臻成熟，并将形成可用于管理技术系统相关企业风险的工具。SIM 产品中的一些新增功能将包括：IT 系统的业务相关性；IT 系统的商业价值；以完整性、可用性和风险价值为基础的服务水平及业务连续性视图；以职能为基础的工作流程告警；以及通过融合系统和业务流程视图而评估的企业风险等等。

简言之，新的 SIM 产品将使企业的多个不同部门都能管理整个企业中的企业风险，包括法律、财务、审计、IT 运作、IT 规划、人力资源（HR）以及企业规章制度等职能部门所涉及的不同形式的风险管理。除安全事件之外，在 2003 年，新的 SIM 产品还将覆盖更大的范围，因为这些 SIM 产品将进一步包括电子邮件、万维网服务器等最常用的应用系统、数据库和普通应用网关。

本白皮书主要探讨 SIM 的现状，分析 SIM 早期部署的一些驱动因素，介绍 SIM 中所添加的一些新功能，阐述 SIM 作为以 IT 为基础的、一致的企业风险管理惯例平台的作用，并深入分析为什么说 SIM 能给企业带来更大的价值。

SIM 的驱动因素：资源匮乏、工具短缺及安全信息过多

安全信息过多是 IT 机构所面临的最大问题。

导致人们对 SIM 感兴趣的主要因素包括：IT 人力资源不足、缺少可用于自动收集和分析安全事件的工具，以及安全信息过多等。

其中，安全信息过多是IT机构所面临的最大问题。而导致安全信息泛滥的最主要原因则在于，IDS、IDS 检测设备、网络路由器和防火墙等安全网关总在收集着极大量的数据。

遗憾的是，这些网络设备所收集的大多数安全事件数据都是噪音。Cisco 公司去年进行的调查表明，网络网关每个月所收集的安全事件的数量超过成千上万条。这些数据中近 90% 都是与安全关系不大而且与企业风险也毫无关系的、未经过滤的背景“噪音”和杂音（图 1）。

IT 高级主管和安全专家们普遍认为，最大的问题包括：

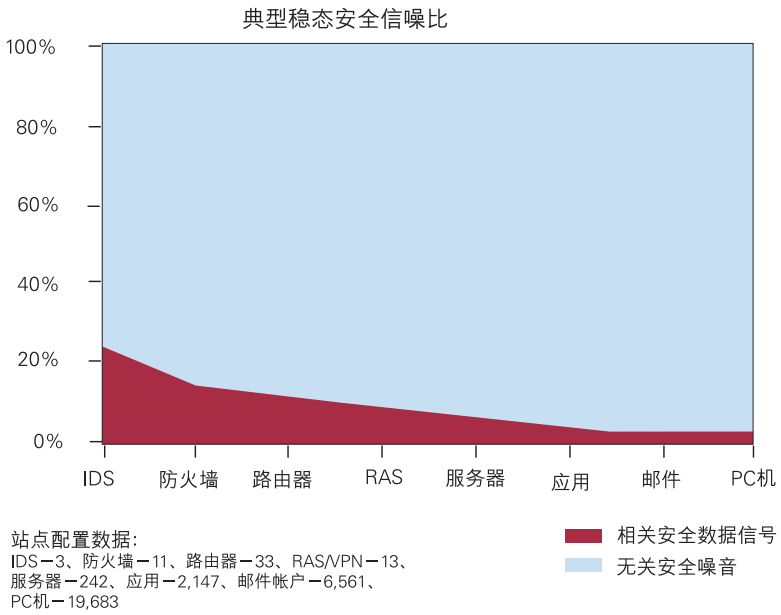
- 安全审计信息日趋泛滥，对“网络”设备的影响非常严重。
- 人们往往无法访问或很难获得本地商业系统中所包含的审计数据。
- 人们几乎不可能从背景“噪音”中识别出企业风险。

事实上，安全信息过多的问题已经远远超出了企业所能处理的限度。即使企业可以雇佣足够多的人手来具体解决每一个安全事件，但仍可能会劳而无功：这不仅是因为雇佣更多人手是对资本的低效利用，而且还因为，电子、数据位和字节的流动速度总是要比人的操作速度快得多。人力资源匮乏、信息泛滥、工具短缺，所有这些问题均可通过 SIM 应用来加以解决，而且，这些 SIM 应用还能处理极大量的安全和审计数据，帮助我们从这些数据中发现问题，使企业只需配备很少量的人员就能充分利用其中的自动化技术和功能。

推动 SIM 应用发展的事件数据和技术基础

任何“事件”都会推动 SIM 应用的发展。安全网关供应商们一直在试图使 IT 买家们相信，“网络事件”与“主机事件”是不同的。在 IDS 检测设备供应商争先恐后地抢占市场份额的 1990 年代末期，这一差异化营销手法已经登峰造极。因此而产生的市场营销炒作一直陪伴我们走到了今天。

图 1
安全信息的泛滥



目前的技术现状是，IDS 检测设备、路由器和防火墙等网络设备也都是主机，尽管它们都是针对特殊目的而建立的主机。而且，它们的特殊目的主要是针对网络服务、端口和协议的。无论其来源是什么，为SIM 应用提供数据的审计和事件监控设备的核心模块都是以外围事件触发器为基础的，其中就包括了多种不同的技术。这些技术包括 签名模式、数据库审计掩码、应用日志、SNMP 陷阱和 RMON（远程监控）事件等。

从 SIM 的角度看，每一个 IT 应用和设备乃至漏洞及威胁数据库都会产生丰富的事件数据，而且，这些数据都可以帮助我们发现基于价值的风险。就此而言，产生数据的来源无论是“网络”事件还是“数据库”事件，无论是 “应用”事件还是连接到网络的专用主机，或者是存储着已知漏洞和威胁的数据库，SIM 都是不变的。SIM 应用可对任何事件数据的类型、来源和内容等进行智能化分析。虽然 SIM 应用考虑到了 IT 设备和数据集的特殊目的，但 SIM 分析可以不考虑收集数据的来源和方法。而且，它也必须不考虑，因为数据和噪音的数量会随时间而不断增多。

早期的 SIM 系统：2003 年以前

SIM 系统于 1999 年首次面市。在此后的四年里，开发商为这些系统开发了一整套可存放在本地设备上的代理，这些代理有很多功能，如收集安全事件数据、连接到最常用的网络安全网关——包括 IDS 检测器、防火墙、网络路由器和某些 VPN 路由器等。

在很大程度上，这些系统主要（且几乎只）用于安全事件数据的收集、融合和关联。早期 SIM 产品可在整个企业网络上提供相关联的数据和显示服务等，但仅限于安全事件的数字化、表格化和图形化显示（图 2）。

经过发展，这些产品已经不仅仅能实现基于网络的安全事件数据的平面显示，而且还提供了意义更丰富的图形和告警服务。其中有一些还包含了彩色代码图形，可通过不同的优先级来帮助 IT 管理人员进行响应和协调工作。很多早期 SIM 产品都包括了可根据概念风险形式来分析网络安全事件数据的应用。然而，早期 SIM 产品也存在若干缺点，如:

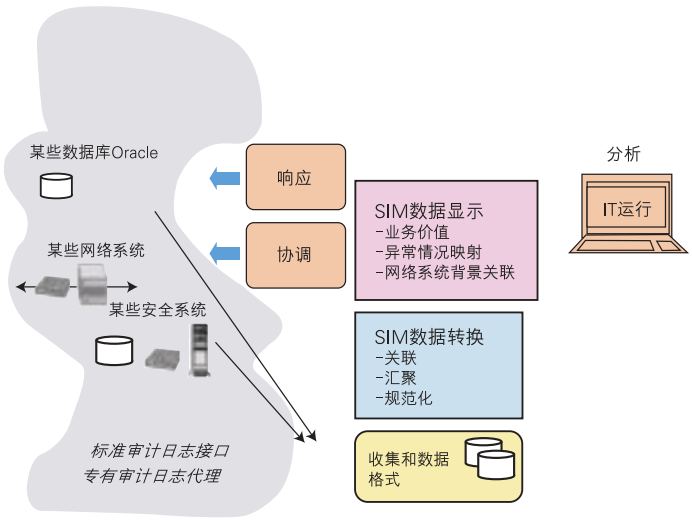
- 不能根据企业具体情况对安全事件数据进行价值调整。
- 必须依靠技能非常熟练的网络安全工程师来解释结果。
- 没有考虑基于 IT 的网络事件以外的风险。

虽然对 2003 年以前的 SIM 系统的这一概括并不具有普遍性，但多数系统都在这一概括的范围内。然而，在 2002 年期间，很多领先的 SIM 供应商开始倾听客户的意见，也开始采取措施来满足客户需求。2003 年已经和将要面市的产品中就体现了这种趋势。

基于 SIM 的安全管理系统：2003 年及以后

SIM 应用能处理输入到其中的大量的、无论任何形式的事件数据集，包括与企业网络相连的任何来源乃至任何已知漏洞和威胁数据库等所产生的实时事件数据。2003 年，领先的 SIM 系统可评估被管理 IT 资源的资产价值、这些资源及其相关企业流程的商业价值、这些资产遭受威胁时的企业风险，以及这些 IT 资源不可用或受影响时对企业造成的风险。

图 2
2003 年以前的早期 SIM 系统



将 IT 安全转变为有效的企业风险管理

到2003年，通过关注于企业资产价值、威胁和漏洞的交汇点，SIM解决方案能帮助企业超越技术控制管理，进而实现积极的企业风险管理。

通过关注于企业资产价值、威胁和漏洞的交汇点，基于SIM的安全管理将使企业进入积极的风险管理新境界。

除了在SIM解决方案的分析组合中添加业务价值、威胁和风险以外，某些SIM解决方案还可在插接兼容层中实现可视化和告警输出功能，因此可将可行性相关信息传递给整个企业中的人员。这样，不同业务和职能部门——包括人力资源、法律、审计、IT、财务以及规章制度等部门——就能实实在在地通过独特视图来分析各类风险（图3）。

SIM 数据的收集与格式

SIM 应用是依靠数据而运行的：数据越多越好。数据越多，寻找事件之间的关系就越容易——也越快速。早期SIM 系统的用户显示，此类系统的应用可借助信息泛滥而成长，并可帮助人们摆脱这一负担。虽然某些SIM 解决方案只能从安全设备中收集数据，但其他此类解决方案却能使用几乎任何记录方案所产生的、基于安全和审计的事件数据，包括本地审计文件、主机、大型机、Unix 和 Linux 系统、Windows 系统、应用、数据库、Web 和邮件服务器、网络设备、IDS 检测器、防火墙乃至网络路由器等。SIM 的数据来源还可包括 SNMP 供给、RMON 陷阱，以及用于提取任何审计相关数据的具体应用编程接口（API）。

通过寻找和确定不同网络、系统、应用及交易系统上事件数据之间的关联，SIM 能更快速地识别并提醒相关人员注意那些可对企业业务运作产生直接影响的风险。SIM 超越了“网络安全事件数据”的范畴，其分析应用不但注重技术，而且还可对企业产生积极的影响。

基于 SIM 的分析引擎

数据转换和分析是目前市场上多数SIM 应用的核心。用于将“事件”数据转换成有意义的信息的主要工具包括：数据规范化、融合和关联等应用。

目前，SIM 产品的多数供应商都对事件数据进行规范化处理，以确保其分析应用——融合和关联——能以相似的方式处理数据。进入 SIM 系统的多数事件数据均根据其来源进行不同的格式化。这些不同的格式有些类似于Microsoft Word的一个版本与另一个版本的数据格式之间的差别，只不过，这里所规范化的数据是“事件”数据，而不是文字处理文本。我们还可以从另一个角度来看待数据规范化，即它可将多种“事件”数据语言翻译成 SIM 应用所通用的世界语。

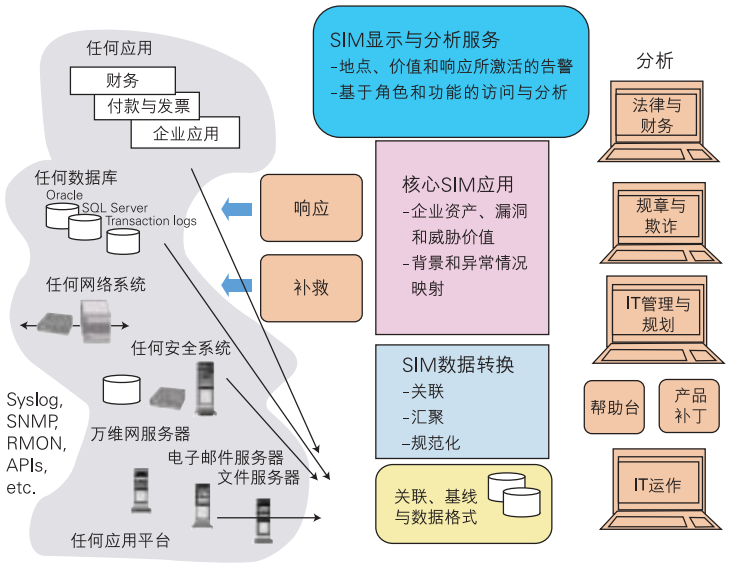
几乎所有SIM解决方案都会对事件数据进行融合。数据融合功能可获取规范化数据，并可按类别对其进行组织。例如，这些类别可以是来源（IT系统、应用等等），以及资产价值或业务职能等。SIM 融合功能可获取相似类型的事件数据，然后将其复制到多个类别之中，让更高层的应用来处理。

多数SIM 应用可实现三大类关联，即：规则关联、异常关联和统计关联。基于规则的关联可将预先打包的转换事件数据提供给数据的不同“视图”。例如，规则可以按照与某个具体交易操作、某一类交易和某个地理地点等准则相关的所有事件对数据进行详审。基于异常情况的关联往往要依赖于SIM 系统所创建的被测量事件数据库，以及从该数据库的“学习模式”中收集的一组“基线”数据。“基线”快照一般会运行几个星期，然后与当前事件进行比较，以确定是否正在发生与基线

不同的异常情况。将来，要想为不断变化的IT环境和商业交易环境创造价值，基线捕捉功能就必须在启发式的稳态模式下工作。

目前，统计关联技术可提供有用的信息，特别是针对基于时间的事件。然而，除基于时间的事件之外，统计关联目前也是很多买家和供应商的学习过程。幸运的是，人们也在根据一般采用假设检验和统计分析的内部审计团队所提出的要求，在 SIM 中添加新的应用。

图 3
以企业为核心的 SIM 系统，2003 年及以后



SIM 显示与分析应用

几乎所有的SIM 产品都能提供强大的显示和可视化功能，使人们能“看到”大量数据中众所周知的蛛丝马迹。SIM 产品一般可提供不同的数据视图，包括：关于整个企业网络的可视化视图、关于具体应用服务器的深入视图、关于以规则为基础的相关数据的交叉视图，以及可显示与最优风险水平不同的统计视图。需要考察的一些更新特性包括：彩色代码告警、风险预测、政策偏差、地理地图、地形投影、体系结构映射、应用装载、交易中的异常“显示点”、建筑物出口，以及电子系统访问点等。SIM 还可实现关于以企业为基础的风险的视图，如“对企业的影响”和“攻击的可能性”等简单而有效的视图，使企业能更轻松地根据自身的独特需求来安排纠正措施的优先级。

聚焦业务价值与 SIM

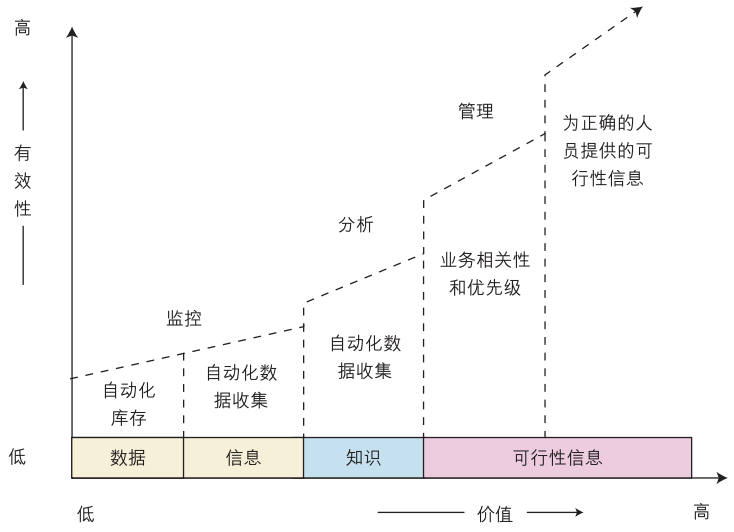
基于SIM的风险管理工具之所以能提供关于企业风险的更新视图，是因为它们能将IT系统的业务价值映射到机构之中。这一排序一般是按业务职能来简化的，因此，可以将价值关联到多种不同的IT资源、应用和数据。例如，在自动发现后，某些SIM 应用可为用户提供机会，让他们用颜色代码标识出在世界各地用于客户服务、制造、分销、订单处理、开票、信用操作、销售、会计、人力资源和其他业务职能的多种不同的IT系统。然后，机构会根据担任不同工作的不同人员所履行的职责为这些“业务职能”赋予“价值”。

通过比较业务职能部门所使用的IT系统，并向这些系统赋予商业价值，企业就能将其响应和补救工作集中在优先级较高的业务需求上。SIM 并不是对每个事件都给予同等对待，而是根据技术的商业用途，对事件数据给予某种“企业风险”的区别对待，因此能为机构带来更大的价值（图4）。通过按企业风险和优先级来绘制交叉表格——如果这些系统不可用或受到影响的话——SIM应用就能将与企业相关的优先风险与可稍后再解决的非紧急信号和事件区别开来。

按相应工作职能访问 SIM 数据的视图

SIM 的一些新应用可根据工作职能，并通过有预配置应用和数据权限的可视化门户等提供事件数据的视图。虽然IT机构的安全管理员可以处理防火墙、IDS检测器和网络路由器等所产生的安全事件，但他们却不应该访问与财务记录和客户记录相关的数据，以及其他机密的商业交易数据。

图4
SIM的价值：为正确的人员提供可行性信息



同样，也可以为规章制度部门的管理人员提供与其工作相关的数据，同时，还可以为审计人员提供与其职能相关的详细数据，为财务和法律部门官员提供企业相关技术风险的重要汇总视图，这些都不会受数据泛滥的影响。SIM 能提供任何数据，如：风险汇总视图，规章制度部门管理人员、审计人员乃至负责应用、网络、运营、安全以及数据存储系统的IT管理人员所需要的繁杂的数据。

SIM 的一些缺陷

迄今为止，市场上有大约 20 种不同的 SIM 产品和类似 SIM 的产品，在短短四年里，这些产品实现了快速的发展。SIM 技术的发展导致不同供应商的产品之间出现了一些较大的差异。这里介绍买家需要考虑并应将其结合到其评估准则中的一些主要差别和潜在问题。

实际事件数据的收集

某些SIM应用只记录IDS检测器所产生的、与安全相关的事件。其他一些SIM产品则能处理相关网络安全网关所产生的审计数据。还有其他一些SIM系统则能处理网络上几乎任何应用系统所产

生的数据。导致这些差别的原因在于，供应商采用了不同的技术来处理和收集审计事件。其 SIM 产品只收集网络安全事件数据的供应商是在使用这些设备所产生的标准输出日志。这些解决方案往往会要求 IT 管理人员必须部署拦截器代理，因此可帮助 IT 机构克服来自 IDS、防火墙、网络路由器以及相似网关的数据的泛滥问题。然而，网络安全 SIM 系统只能对企业中的这些安全系统之间的数据进行关联。遗憾的是，它们看不见支持企业运转的关键任务商业系统、数据库和应用。这些 SIM 解决方案的分析引擎只能猜测出业务价值，因为，分析引擎所能操作处理的相关数据是不存在的。然而，其 SIM 产品能从任何设备收集数据的供应商也许更可能——或很快将要——提供可将 SIM 转变为有效工具的功能，因此将能管理与技术运用相关的企业风险。

缺乏“开放”的数据来源

所有 SIM 供应商都面临的一个难题在于缺乏一个针对审计和事件记录数据的“开放”和通用标准。缺乏针对威胁、漏洞、审计和事件数据的一个标准格式——在企业所采用的多种不同技术系统上，这恰恰是所有SIM供应商之所以在对所收集的数据进行任何分析应用前不得不投入工程资源对数据进行规范化的原因。

签名模式与实际事件数据

对于那些将要提供完全基于签名模式的解决方案的SIM 供应商，它们所能提供的任何功能都不会超过软件工程师的风险视图。SIM 系统要想真正发挥作用，就必须收集有效的事件数据。如果关于相关联事件的充足信息最终表明，模式匹配总是能实现更快速、更积极的识别，那么签名模式就是有用的。因此，我们应该认为，签名模式是对有效事件数据的补充和增强，而不能完全取代实际情况。

超越卡目录

目前，某些 SIM 解决方案尚不能自动进行企业风险分析，这是因为，它们的分析引擎尚未考虑到被监控 IT 系统的业务价值。虽然这些“卡目录”型解决方案可以解决 IT 机构中的很多问题，但是，它们的基础融合和关联功能并不能恰当地根据“价值”来区别事件数据。要想超越卡目录，这些解决方案就必须再增加一些功能，如:

- 根据工作职能提供事件数据的多个视图;
- 基于价值的分析应用;
- 覆盖范围更广且不仅局限于安全事件的数据来源。

超越安全事件数据

目前，有几种领先的 SIM 产品可从主流应用系统中收集事件数据，这些系统包括: 电子邮件、万维网、人力资源、财务、交易和客户关系等。到 2003 年，很多 SIM 解决方案将在其产品组合中增加必要的事件收集和业务价值分析等功能，进而使 IT 人员能对一些选择进行比较。

SIM 的其他发展: 迅速普及

今年，供应商们都在纷纷增加新的功能，除了能对企业的安全和风险管理流程进行工业化处理之外，还有望能更大幅度地提高 SIM 的价值。

SIM 可望实现的一些新特性包括:

- 能连续重建 “正常形态” 的综合性 “学习模式”;
- 能在生产环境中运行 SIM 并在部署前检验更改的主动和模拟 “模式”;
- 针对资产价值、事件、风险、漏洞和威胁数据集的开放来源;
- 与用于修复和补救的任何系统相集成。

随着针对 “开放式” 审计事件记录数据的新标准的出台，IT 买家将能更容易地找到选择余地更大的、以企业为核心的先进 SIM 解决方案。“开放式” 行业标准事件收集方法将使供应商能够将工程资源重新分配给分析和显示服务，而不是将其用于可能需要配备的、旨在收集数据的很多专业代理。

此外，根据用户的工作职能，供应商还将为基于 SIM 的风险分析增加图形丰富的、新的视图。随着这些新功能的推出，买家将能够以图形方式 “点击” 企业 IT 基础设施的某些完整部分，将其拖放到 “价值” 和 “风险” 区域中，而这些区域则可以表明企业是如何进行经营的，以及企业是如何看待这些运作的价值的。

SIM 的新特性不仅能实现预定价值概念，而且，还可使每个企业都很快地将 SIM 结合到其机构的企业风险管理环境之中。此外，有了以企业为核心的多个风险 “视图”，企业中的多数普通风险管理职能部门还能利用更准确的信息，把它们的工作做得更快、更好。

在 SIM 系统中添加的这些新功能，特别是通过可视化方式来说明对企业的影响与威胁，都表明，企业将能测量并有效地降低其业务经营中所产生的风险。企业将不再被局限于简单的风险技术视图，而是将能立刻看到其业务价值。因此，SIM 的这些新功能将帮助企业有效地将技术的使用所导致的企业风险降低到可接受的水平（图 5）。

Cisco 公司的结论

据 SIM 用户反映，到 2003 年，SIM 解决方案提供的新功能将实现更大的价值，包括:

- 可实现对 “风险状态” 的测量和可视化;
- 可提供经过实践检验的降低风险的措施;
- 可确定威胁和漏洞的优先级;
- 风险事件更接近 “实时”。

虽然过去只注重于安全事件，但是，到 2003 年，SIM 系统将使 IT 行政高级主管、财务主管、法律顾问、内部审计团队、董事会、高级主管人员以及高级业务管理人员等更容易地查看和管理有形风险。此外，到 2003 年，SIM 中的新增应用还可使 IT 管理人员提高被管理系统和网络的服务水平。

到 2003 年，SIM 系统将提供新的业务视图，到那时，只有那些最重要的事件才需要得到立刻关注和修复。 “以企业为核心” 的 IT 风险视图将使审计、法律、人力资源、业务和 IT 等人员利用更少的资源实现更高的效率。

将 IT 安全转变为有效的企业风险管理

SIM 系统目前的用户显示，他们预见到这样的一天很快就会来到，即随着这些安全和风险管理解决方案的完善，他们的机构将注重于解决与用于经营企业的技术系统相关的真正的问题和风险。这些企业都在计划将其主要开支从技术运用转移到风险管理，所以，它们将能很好地扩大用于经营企业的、基于 SIM 的风险管理的范围，这是因为，他们将能应对乃至预测与技术使用相关的企业影响和风险。

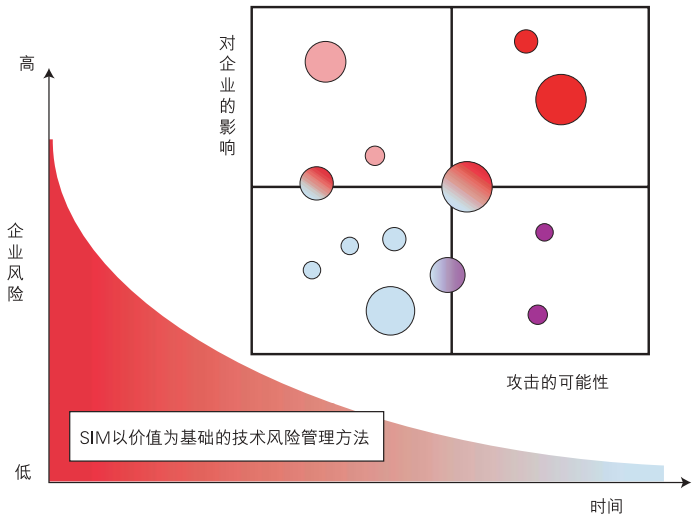
到 2003 年，随着基于 SIM 的风险管理的发展， IT 买家和供应商都将面临一个分水岭。买家将能通过 SIM 实现以企业为核心的价值分析，这将帮助 IT 机构的安全部门走出黑暗，立足于以经验为基础的科学分析，并借此来推动企业的发展。此外，SIM 还将提供这样的数据，即可使买家根据企业需求而非猜测来更妥善地决定应该将富余资金用在风险管理的哪些方面。买家应该寻找在业务价值资产应用、信息管理以及“开放式”安全系统等领域中具有专业技术和知识的供应商。

对于供应商而言，SIM 有望将行业环境重新协调到与当前情况不同的方向上。虽然这对于某些人而言将是艰难的，但是，对于那些有足够远见、能认清 SIM 将产生的影响的人们，他们将能满足更明智——也更务实——的客户需求。

对于那些已经熟悉基于 SIM 的安全管理新应用的内在业务价值的人而言，他们也都在计划尽可能更充分地加以利用。

而对于那些尚不熟悉 SIM 的人而言，就在今年，他们也都将在别人的帮助下，了解其他企业或同事都知道什么，以及他们为什么计划要充分利用这一系统。

图 5
将 IT 安全转向企业风险管理



思科系统（中国）网络技术有限公司

北京
北京市东城区东长安街1号东方广场
东方经贸城东一办公楼19一21层
邮编：100738
电话：(8610)65267777
传真：(8610)85181881

上海
上海市淮海中路222号
力宝广场32一33层
邮编：200021
电话：(8621)33104777
传真：(8621)53966750

广州
广州市天河北路233号
中信广场43楼
邮编：510620
电话：(8620)87007000
传真：(8620)38770077

成都
成都市顺城大街308号
冠城广场23层
邮编：610017
电话：(8628)86758000
传真：(8628)86528999

如需了解思科公司的更多信息，请浏览http://www.cisco.com/cn

思科系统（中国）网络技术有限公司版权所有。

2004 ©思科系统公司版权所有。该版权和/或其它所有权利均由思科系统公司拥有并保留。Cisco, Cisco IOS, Cisco IOS标识，Cisco Systems, Cisco Systems标识，
Cisco Systems Cisco Press标识等均为思科系统公司或其在美国和其他国家的附属机构的注册商标。这份文档中所提到的所有其它品牌，
名称或商标均为其各自所有人的财产。合作伙伴一词的使用并不意味着在思科和任何其他公司之间存在合伙经营的关系。