2008 年 10 月

成本、复杂性及风险：未来企业的安全

目录

简介

根据 IBM 标志性的《 全球 CEO 研究 》，“未来企业”[1]首席执行官及其他高级业务主管预测：变革将带来并推动激动人心的全新业务环境，包括新的业务设计、突破性创新和持续性经济全球化。作为 CIO，您有责任将 IT 应用、服务和基础架构转化为灵活的自动化环境，这将能够使贵企业充分把握充满活力的市场所带来的机遇。

与许多 CIO 一样，您可能感到 IT 安全性与合规性会成为实现此构想的最大障碍。毕竟您所处的位置使您能够看到，技术变革的力量已推动安全性/合规性的成本和复杂性不断攀升。变革很容易被视为安全的对立物，然而未来却充满着更大的变革。诸如“如何全面掌控风险管理和业务延续性？”和“当安全性与合规性仍然是难以揣测的目标时，如何提高适应能力并有效平衡风险、复杂性和成本？”之类的问题将被放到第一位。也许您希望所有安全性与合规性问题彻底消失。

长期以来，安全技术的开发和部署一直与 IT 基础架构的主流、应用和流程脱节，供应商很少关注如何将其集成到主流技术当中，也很少关注其增加业务流程复杂性的程度。所以，安全性与合规性成本继续以 IT 预算增长速度的三倍速度增长也就不足为奇了。

要点

CIO 必须成为未来企业变革的代言人，同时也必须能够处理变革对安全性与合规性的影响。

未来企业需要对安全性与合规性解决方案的构思、应用和管理方式实施重大改革。这就要求贵企业寻找新型安全合作伙伴。这类新型合作伙伴（也称为改革型安全供应商）将具有安全行业中长期缺乏的强大供应商领导力。这种领导力将包括一流的安全专业技术、广泛的 IT 专业技术，以及支持安全性与合规性新构想所需的深厚资源与承诺。

您和您的组织将共同分享和实现这一全新构想。改革型安全合作伙伴将与您紧密协作，共同应对三项挑战：1）重新定义并简化风险管理，以便为如何在不断变化的环境中平衡风险、复杂性和成本提供更明确的指导；2）提供全面的安全框架和组合，包括领先的安全性研究、安全产品和安全服务，这能够为部署无缝集成和业务驱动的综合安全解决方案提供最大的灵活性；3）缩短并简化风险生命周期，从而降低长期安全成本和复杂性。

最终，这种改革将安全技术紧密集成到现有的 IT 基础架构和业务流程当中。这将使安全性作为企业资产得到更好的控制，并有助于简化安全性与合规性、降低其成本且使其更能适应不断变化的业务需求。

趋势：变革的力量使得 IT 安全性/合规性变得昂贵而复杂

融汇到安全“完美风暴”中的五种主要变革力量正不断改变风险环境，而风险环境又转而不断增加复杂性和成本。

要点

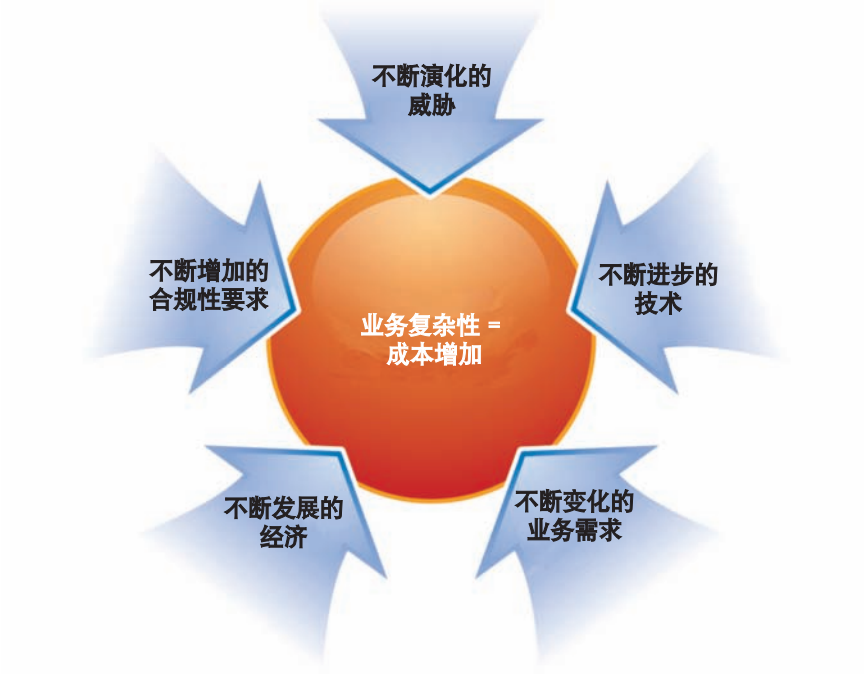

图 1：五种主要的变革力量

多种变革力量（企业内部和外部）直接影响着安全性与合规性的成本和复杂性。

1. 不断演化的威胁

它并非一直如此复杂。二十世纪八十年代和九十年代的大部分时期，IT 安全性主要包括防病毒和防火墙技术。这种相对狭窄的技术关注点占据着安全预算的很大部分。但近年来，安全威胁已经显现出一种整体格局，从拒绝服务攻击，到 rootkit、僵尸网络（botnet）、基于浏览器的攻击、网络钓鱼（spear phishing）和网络捕鲸（whaling），种类繁多。IBM Internet Security Systems™ X-Force® 威胁报告中详细介绍了这种快速变化的格局。[2]威胁的本质也已从恶作剧发展为带有政治色彩并显露出利益驱使的动机。许多新型威胁已衍生出新的独立代理或需要专家部署和管理的应用程序。许多此类解决方案已逐渐标准化并嵌入到交换机、服务器、操作系统和其他基础架构组件中，但同时新型威胁也不断出现，这就要求对新技术进行新一轮的资本投资。这些新技术的资金必须从预算中筹集，然而现有的安全解决方案成本已经造成预算紧张。

图 2：日益增多的威胁种类

2. 不断增加的合规性要求

与安全相关的法规和企业的行业合规性负担也在不断增加。这些要求所针对的目标形式多样，包括行业、国家/地区和州。在许多司法辖区中，不遵守法规将使企业面临民事和刑事处罚的风险。因此，对高级管理者而言，合规性无疑是在制定预算时的优先议题，通常优先于相同资源池中的其他安全方案。

3. 不断进步的技术

虚拟化、Web 2.0、以服务为导向的体系结构、云计算和其他技术的发展不断拓展着企业的业务边界，并建立起业务互动的新领域。此类突破性创新同时也带来新的风险和/或逐步破坏原有的安全模式和安全投资，这就要求新的应对措施，并因此产生新的成本和 IT 管理挑战。

要点

4. 不断发展的经济

全球化经济的动态发展逐渐使安全预算变得紧张。华尔街和世界金融市场近期的波动已充分表明全球化在加速并扩大经济影响因素（从原油处理和抵押贷款利率到货币兑换率）方面的重要作用。即使没有最严重的波动，全球经济也正迫使 CIO 调整安全性与合规性战略及运作。例如，外国政府提出独特的法律法规、全球业务运作要求的 24 小时工作日，以及安全解决方案必须适应形形色色的地域、语言、法律和文化因素要求等。

5. 不断变化的业务需要

许多公司越来越需要进行快速调整，以适应不断变化的市场环境。这有时意味着此类调整战略将随着兼并、收购或分布方式的变化而变化。或者也可能只需要采用创造性的方式来应用技术、人力和其他资产，以提高内部生产率，改进与供应商的协作并增强与客户的交互。因为所有这一切通常都包括潜在敏感数据的共享，所以会影响风险态势。

CIO 的迫切需求

平衡风险、复杂性和成本

上述所有变革力量使得安全性与合规性在制定计划和预算时成为变幻莫测的难题。

对 CIO 而言，不断平衡变幻莫测的风险、成本和复杂性可能会产生安全疲劳，并最终导致做出不恰当的选择。

因此，尽管 IT 安全性/合规性对业务极其重要，但通常仍被视为一种干扰和管理负担，而您可能希望它彻底消失。但由于它是 CIO 不可推卸的责任，所以您必须找到可用预算、可管理的复杂性以及可接受的风险这三者之间的隐形平衡点。这五种主要的变革力量将使平衡风险、复杂性和成本变得异常困难，而这在很大程度上也是您的责任。

数据和 IT 基础架构的业务价值已达到前所未有的高度。作为 CIO，您必须运用越来越多的安全措施来保护这些战略资产。但安全性仅是您工作的一个方面；您还需要负责大量 IT 相关的其他工作，且资源有限。

由于安全性与合规性挑战的复杂性和残酷性循环，CIO 容易出现“安全疲劳”，并常常会走捷径以求降低成本和工作量。

在某些情况下，这可能意味着仅仅为了以尽可能低的成本通过合规性审查而采用某种解决方案，而并不足以缓解风险。在其他情况下，CIO 可能会选择通过减少供应商的数量来降低成本，而通常对特定供应商的产品和技能是否符合业务需求欠缺深入分析。

几乎任何针对成本采取的措施都会对复杂性和风险产生一定的影响。

图 3：降低复杂性成本的措施可能会提高风险级别

在不牺牲安全性或进行“有效简化”的情况下，采用有效方法简化解决方案来平衡风险、复杂性和成本仍然是一个难题，然而以特定方式应对风险和法规环境的持续变革，必然会牺牲安全性。目前，在压力下做出的快速修复决策也许能够满足短期预算的需要，但它无法完全解决许多可能存在严重隐患的风险。

那么，如何才能简化平衡方案呢？如何才能使抉择更为明确、更倾向于目标驱动呢？我们必须考虑安全供应商的作用，以及他们对当前困境所能贡献的力量。

供应商责任

当涉及到风险、复杂性和成本的适当平衡时，资金最终会成为 CIO 和 CISO 的最大阻碍。但在很大程度上，造成与 IT 安全性与合规性相关的挫折和困扰，责任应由安全供应商承担。多年来，专营安全产品的公司开发出的新技术复杂而缺乏与现有 IT 系统的互操作性。开发出此类解决方案的供应商缺少针对您的利益而简化产品和降低花费的积极性。

而承担“安全供应商”责任的基础架构供应商则一直等到安全解决方案成熟并大量商品化之后，才最终将其作为功能捆绑到交换机、服务器和应用程序中。在提供最新技术或提供有关安全性与合规性战略的专业指导方面，他们通常缺乏应注重的专业技术。

迄今为止，没有任何领域的供应商能够担负起在整个 IT 安全风险生命周期中降低总成本和复杂性的责任。您已经自己承担了大部分责任。现在是让我们期待并要求供应商承担更多责任的时候。

要点

未来企业需要对安全性与合规性进行变革，使其从抑制技术转换成使能技术。

应对未来企业的安全挑战

在 IBM《全球 CEO 研究》的附录“未来企业 — 对 CIO 的启示”中已经对您所面临的挑战进行了总结。根据该文件的叙述，CIO 将负责“在企业范围内作为 CEO 重要同盟以及在自己的 IT 组织中，以‘变革领导者’的身份推动改革，以‘变革代言人’的身份实施改革。”

作为 CIO，为了适应并帮助创立未来企业，您需要帮助调和变革的内在冲突。变革确实可以成为推动增长和机遇的力量，但它也会带来风险，使得安全性与合规性成为您最苦恼的负担。

要降低业务成本和复杂性，在面对变革时风险与合规性管理必须具有更好的可持续性和业务驱动一致性。因此，安全性作为一种 IT 规范，必须进行变革 — 从限定禁止行为的抑制技术，转换成能够让您满足任何需求以实现业务目标的使能技术。

这是一项浩大的工程。尽管作为企业内的变革代言人，您能够完成许多工作，但安全性与合规性的真正改革还需要各类不同的安全供应商。

改革型安全供应商的出现

未来企业需要的供应商，应具有一定规模并努力担负起安全行业中的改革责任。与任何传统类型的安全供应商不同，改革型供应商将在 IT 主流应用中引入安全技术，并对全部风险生命周期承担责任，要做到这些，它必须具备以下特征：

- 通晓 IT 基础架构各方面的专业技术
- 安全产品研发领域的领导地位
- 安全产品和服务的深度和广度
- 广泛集成专业技术以及业务咨询
- 将技术与业务流程结合的专业技术
- 全球化服务
- 融资优势和持久力

要点

改革型安全供应商必须提供更为广泛、业务驱动的成套解决方案，且必须具备市场领导力并承担责任。

改革型供应商必须灵活运用这些优势，以便应对以下三项主要挑战：

1. 重定义和简化风险管理，以适应持续的变革

如本文前述的介绍，风险态势的不断变化带来日益增长的安全性与合规性需求，这些需求必须与静态预算进行权衡。由于 CIO 面临着清楚而全面地审视威胁态势的挑战，且他们在安全决策方面缺乏指导，因此，他们常常会建立以虚假的经济状况为依据或与实际业务目标相分离的优先级。出现这种问题的部分原因，仅仅是由于对五种主要变革力量影响风险的多种方式缺乏了解。传统的供应商只能提供单一变革因素的信息，很少能够洞察更多因素。

要提供注重业务的完整框架以便评估安全需求和开支优先级，改革型供应商必须以高度精炼和动态的方式重新引入企业风险管理。这将需要考虑所有的主要变革因素，并且将包括基准流程、成熟度模式、行业最佳实践和其他元素，以便在评估风险对实际业务目标的影响时制成更完整和更准确的企业风险档案。

这是一种连续且具备适应性的风险管理方法，它可以避免安全性与合规性计划和管理过程中的大量压力和猜测。通过实施更加智能化的业务驱动决策，让您不仅在现在，而且在将来也能够更好地控制与安全相关的成本和复杂性。

2. 提供安全框架和组合，从而形成以业务为中心的无缝解决方案

传统上，安全技术均为隔离开发，直接用途范围不广，并且仅在大型 IT 基础架构中很小的领域内应用和管理。在向未来企业发展的过程中，这种方法并不可靠。主要的风险挑战（例如支付卡行业数据安全标准）要求多个安全领域中的技术，这些技术必须能够集成到企业基础架构的重要部分和关键业务流程中。如果综合解决方案必须与多种来源的技术组合在一起，则不能考虑成本和复杂性。

改革型安全合作伙伴必须提供无缝且有效的安全性与合规性的完整解决方案。首先，这意味着需要涵盖以下五个主要安全领域的有效安全产品的深层组合：

1. 人员与身份
2. 数据与信息
3. 应用程序与流程
4. 网络、服务器与端点
5. 物理基础架构

其次，改革型合作伙伴必须能够提供满足您独特业务需求的解决方案。这需要丰富的业务和应用程序知识，以及将完整的技术解决方案紧密集成到独特基础架构环境和业务流程中的资源。

最后，您的合作伙伴必须处于安全产品研发的最前线，这样才能使您的安全性与合规性构想具备前瞻性，从而确保变革的力量不会超出您抵御风险的能力。

图 4 提供完整安全生态系统的简化视图。

图 4 提供完整安全生态系统的简化视图。

图 4：总体安全框架

3. 缩短和简化安全风险生命周期

安全性是产品还是功能？在整个风险生命周期过程中，安全性即是产品，也是功能。如图 5 所示，任何特定风险的解决方案通常在其生命周期开始时都可能是昂贵且复杂的离散独立安全产品。在大多数情况下，解决方案都会经历过渡阶段，在此期间它将日益标准化并最终成为集成到 IT 基础架构中的一项功能。作为 IT 基础架构的嵌入式功能，安全产品趋向于成本更低、更成熟且功能更加自动化。

改革型供应商将缩短并简化由产品至功能的生命周期，以便使您更好地控制安全成本和复杂性，即使在变革的力量不断改变风险态势时也不例外。

首先，这意味着生命周期的“过渡”阶段发挥更为积极的作用，即通过有效的集成技术、中间件、合作伙伴关系和沟通能力推动安全解决方案更快进入“功能”阶段。

要点

今后，越来越多的安全性与合规性解决方案必须从一开始便无缝集成到现有的 IT 基础架构和业务流程中。

其次，从长远来看尤为重要的是，改革型合作伙伴将通过设计提供更紧凑的生命周期。随着产品开发、安全性和基础架构技术集成和管理能力的不断提高，新型合作伙伴将从两方面加快此过程：1）在基础架构系统中不断添加更多安全功能和安全框架，以及 2）尽可能在设计时集成安全解决方案，或建立能够使安全技术更易于集成到现有 IT 基础架构和管理系统中的解决方案体系结构。

最后，改革型安全合作伙伴将努力使贵企业在安全改革的突破性创新中得到缓冲，并通过将许多安全性与合规性解决方案作为托管服务，来提供更大的战略灵活性。

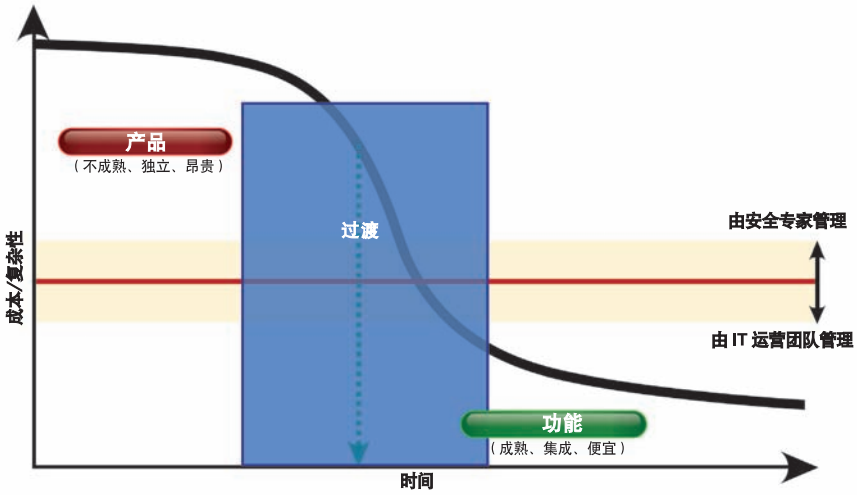

图 5：风险生命周期中成本和复杂性递减。在大多数企业中，生命周期的各个阶段（产品、过渡和功能）都存在安全解决方案。

结论

未来的安全性与合规性必须适应未来企业的要求，未来企业将面临突破性创新、全球化和其他通常会使安全性变得更加复杂和昂贵的变革力量。最需要的改革是将外来新技术，快速转换成稳定、低成本，并可融入到主流 IT 体系结构中、易于管理的安全功能。

要点

重点在于消除不断变化的风险环境带来的安全性与合规性管理的许多不确定性。

其途径非常清晰明确：将安全性与合规性迁移到现有的 IT 基础架构中，并与标准管理平台和业务流程集成到一起。最重要的是：从整个风险生命周期的角度进行未来风险创新。这种方法本质上是为了降低持续的变化对业务成本和复杂性的影响，并改善业务持续性。

您可能一直忽略了这项任务：贵企业负担不起评估风险态势、集成新的安全解决方案和维护不断变化的风险/复杂性/成本等所有方面需要的专业人员。并且您原来的供应商不具备提供完整解决方案所需的资源。

IBM 是具备全球影响力的强大组织，其远景目标是成为市场中的改革型安全合作伙伴。

IBM：改革型安全合作伙伴

确保此动态环境的安全性是一项非常浩大的工程，需要涉猎广泛且十分专注的供应商。IBM 拥有承担“改革型安全合作伙伴”这一角色的资源、专业技术和构想。IBM 作为您未来企业的合作伙伴，将其作为保护您未来企业的安全供应商是明智之选。IBM 的特征（符合本文前述要求）便是改革型安全合作伙伴所需具备的核心特征：

- IT 基础架构领域的综合专业知识
- 安全产品研发领域的领导地位
- 安全产品和服务的深度和广度
- 广泛集成专业技术以及业务咨询
- 将技术与业务流程结合的专业技术
- 全球化服务
- 融资优势和持久力

IBM 正重新定义并简化风险管理

凭借市场研究和分析、技术开发和在集成业务驱动解决方案方面的实际经验，IBM 能够深刻洞察业务环境中的风险变化。因此，我们可以对您面临的风险进行更清晰、更全面的评估，并提供更有效的安全性与合规性战略。例如，IBM 客户端安全预备方法可以帮助您建立合理的业务驱动基础，以便平衡风险、复杂性和成本。

IBM 提供完整的安全框架和解决方案组合

IBM 提供广泛而深入的解决方案组合。它覆盖五个主要的安全领域，并包括从简单的点解决方案到全面的托管服务在内的各项功能。最重要的是，解决方案和可选交付方案的广泛组合能够为您提供最大程度的控制，从而使您能够根据独特的需求定制战略。

IBM 缩短和简化安全风险生命周期

IBM 安全性与合规性产品规划越来越多地以未来企业的构想为导向，在未来企业中 IT 安全性将能够适应并轻松应对各种变化。在产品研发、战略性收购及渠道和技术合作伙伴的开发中，我们不断努力使安全性与合规性解决方案能够集成到 IT 基础架构和业务实践中，并成为其有效组成部分。

未来企业将以不断变革为特征，充满刺激。它必将迎来激动人心的专业化挑战，尤其是在安全性与合规性领域。虽然这将是个漫长的过程，但有 IBM 的支持，您可以充满信心地坚持下去。

有关详细信息

IBM 通过将安全性/合规性有效集成到 IT 基础架构和业务实践中，从而为企业提供降低风险、成本和复杂性的安全解决方案，要了解详细信息，请联系您的 IBM 市场代表或 IBM 业务合作伙伴，或者访问以下网站：**ibm.com**/cio。

International Business Machines Corporation
Route 100
Somers, NY 10589 U.S.A.

美国印制
2008 年 10 月

[1] IBM《全球 CEO 研究》《未来企业》。**ibm.com**/enterpriseofthefuture

[2] X-Force 趋势报告 - http://www-35.ibm.com/services/us/iss/xforce/midyearreport/

CIW03050-CNZH-00