IBM商业价值研究院

IT经理和CIO不断转变的角色

2010年IBM全球IT风险调研结果

IBM商业价值研究院

在IBM商业价值研究院的帮助下，IBM全球企业咨询服务部为政府机构和企业高管就特定的关键行业问题和跨行业问题提供了具有真知灼见的战略洞察。本文是一份面向决策层和管理层的简报，是根据该院课题小组的深入研究撰写的。它也是IBM全球企业咨询服务部正在履行的部分承诺内容，即提供各种分析和见解，帮助各个公司或机构实现价值。有关更多信息，请联系本文作者或发送电子邮件到ibvchina@cn.ibm.com。
请访问我们的网站：http://www.ibm.com/cn/services/bcs/iibv/

作者：Linda B. Ban, Richard Cocchiara, Kristin Lovejoy, Ric Telford, Mark Ernest

法规要求不断提高，24×7在线业务不断增多，以及经济不确定性的持续影响使得管理各种形式的风险的重要性日益提高 – 包括与业务、数据或者事件相关的风险。2010年IBM全球IT风险调研指出了与IT风险相关的挑战，以及IT经理和CIO更好地了解、应对和消除这一担忧而采取的措施。在被调查的IT经理中，大部分被调查者预计他们与风险相关的职责将会提高。显而易见，IT风险管理的范围非常广泛，而且可直接影响一个企业的竞争地位，以及客户、合作伙伴、法规制定机构和相关利益方所理解的企业声誉。

从业务角度讲，IT基础架构对于支持和保护企业的关键资产和保证适当的治理与合规，以及对于推动业务增长都扮演着日益重要的角色。因此，IT风险管理不再被视为严格的技术职能，而是一项可对整个企业带来直接业务收益的关键管理任务。

为了更好地理解企业如何管理与降低业务风险 – 尤其是IT风险管理 – IBM发起了2010年IBM全球IT风险调研，这是IBM在IT风险领域持续进行的研究项目的组成部分，并且是首个关于本主题的调研项目。

本次调研于2010年5月和6月与经济学人信息部(EIU)合作开展，旨在更好地了解IT经理目前注重的方面，以及从短期来讲，他们认为在何处存在机遇和挑战。未来的调研将深入考察这些方面，并探索所有风险管理团队面临的选项和决策。

本次调研的结果基于对556名IT经理和其企业IT部门的人员(包括131位CIO)的在线调查。调研的区域包括北美洲、西欧、亚太地区、中东和非洲、东欧和拉丁美洲，而调研的行业包括IT、金融服务、医疗/制药/生物技术、制造和政府部门。被调查企业的收入范围是从5亿美元到100亿美元。

“随着IT已成为更多业务运作的核心，IT风险管理并未被提到相应的重视程度。”

西欧旅游行业被调查者

“尽管有人称，技术已经发展成熟，并且已经商品化，但我们看到，技术‘革命’刚刚开始。证据表明，技术对业务的战略价值仍在增加。”

Brynjolfsson、Erik，Adam Saunders
《数字化时代的创新：信息技术在如何重塑经济？》
麻省理工学院。2010年

调研的主要结果是：

- 调查准确衡量IT风险管理现状的代表企业
- 确定推动(或者阻碍)企业风险管理战略的因素
- 发现企业实施新的风险战略、计划和政策的程度
- 了解IT的发展(例如云计算)如何与企业的总体风险战略保持一致
- 考察IT经理不断转变的角色，包括CIO

总体来讲，对于各个地区、企业规模、行业和角色，调研结果大同小异。(在调研中，所有地区都承认IT风险管理的重要性，并且在这个方面努力进行改进)。基本上，调研参与者都表示出对风险管理和合规努力充满信心(见图1)。

同样，尽管超过50%的被调查者表示，他们的预算没有变化，或者有所提高，但36%的人仍需要努力获得充足的资金，用于应对与风险相关的挑战。此外，尽管普遍认为IT风险管理可带来真正的业务收益，但获得高级领导层的支持仍然是被调查者切实担心的一个问题。

被调查者的反馈似乎指出高层管理者对提高IT风险管理水平的看法和从中能够获得的价值之间的脱节。

为改进留出空间

由于认识到有效的IT风险管理潜在的业务回报，许多被调查者都期望在未来三至五年内扩展与风险相关的举措。虽然如此，被调查的企业在许多方面存在明显的区别。只有半数的被调查企业设立正式的风险管理部门(46%)或者拥有精心设计的业务连续性战略(54%)。另外，业务线和其它运作风险问题(例如财务/业务战略)并不是主要的核心区域。

在被要求描述企业控制IT风险的总体方法时，66%的被调查者认为企业在这方面的表现为“良好”或“优秀”。尽管这代表了大部分企业，但超过30%的企业认为在这个方面属于“一般”或“较差”的水平。然而，72%的被调查者称，其企业的风险控制方法在过去12个月内已有改善。

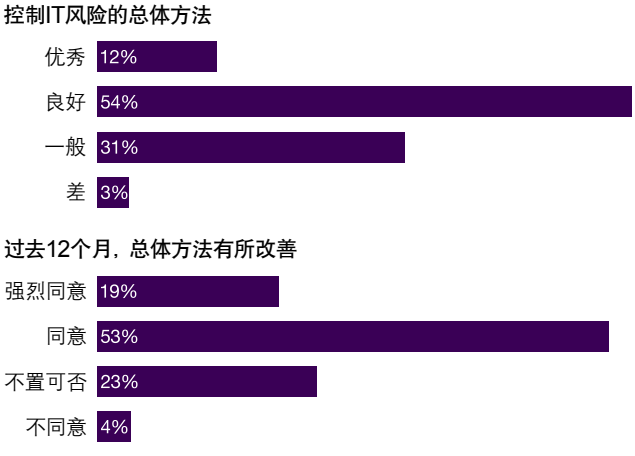

图1. 企业高度关注降低IT风险的方法

“过去，IT组织经过全面的测试后才推出新的IT业务服务，这样做的主要目的是避免业务中断。但现代企业的IT主管需要了解这些测试对业务的真正成本。这不仅包括IT成本，还包括由于业务服务延误而丧失机会的成本。测试所需的每一天都会使创造收入和利润的时间减少一天。如果服务与服务运行带来的收益不平衡，会造成什么风险？”

Mark Ernest，IBM杰出工程师

毫不奇怪的是，47%的被调查者指出，IT风险计划的绝大部分是在孤立的业务部门进行的独立职能。因此，企业了解在哪些方面互相合作是一个严峻的挑战。另外，许多被调查者指出，尽管他们参与了大量的风险管理和合规活动，但他们希望参与更多的活动。(大约一般的被调查者表示他们的企业有风险管理部门，但许多人认为，在传达或者与员工沟通企业的风险管理政策和问题方面，其表现较为落后。)

从积极的方面讲：在严峻的经济环境中，IT风险管理与合规在很大程度上不受预算削减或者节约开支的影响。在被问到企业在2010年的风险管理预算时，14%(80个被调查者)预计这方面的资金投入会大大增加，而39%的被调查者认为会有所增加。36%的被调查者指出，风险管理资金将保持不变。

被调查者认为，IT风险管理的投资可带来巨大的业务收益，主要是在业务连续性(74%)和保护企业声誉(32%)方面(见图2)。被调查者指出，管理IT风险不仅仅是一种防御策略；还可提高企业的敏捷性(19%)，并创造业务增长机遇(12%)，同时降低成本(18%)。然而，大多数IT经理(57%)将时间主要用于处理与基础架构相关的风险。

首要任务：IT安全

尽管IT风险存在于各个流程、活动和系统中，但在被调查的IT专业人员中，IT安全(对于黑客和未授权的访问/使用企业系统的脆弱性)是78%的被调查者最关心的问题。硬件和系统故障排在第二位 – 63%的被调查者指出了这一问题。断电和物理安全(40%)的排名并不太靠后，位于盗窃、产品质量、合规、自然灾害、电子发现请求、供应链故障和恐怖袭击之后。

IT经理对于风险管理的重要性有明确的看法，并且有特定的关注领域。但是，他们对于企业适当地处理和应对风险的信心却存在巨大的差距。例如，仅22%的被调查者认为，其企业已经在IT风险方面做好准备。

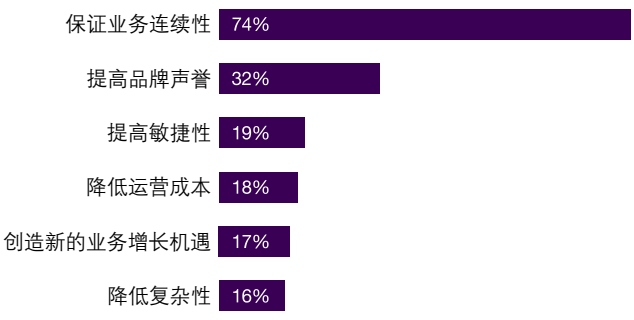

图2. 增强IT风险管理所带来的收益

23%的被调查者对于其企业在硬件和系统故障方面的准备程度持有相同的看法。企业为防止断电提供了更多的支持 – 32%的被调查者指出，其企业在这一方面做了充分的准备。然而，在企业对于应对总体IT风险的重要性和适当地管理和控制风险的能力方面，被调查者的看法存在明确的差异。

“业务连续性不仅仅包括对自然灾害或者可预计的灾害做出规划。它的真正意义在于建立风险意识文化 – 确保拥有必要的工具、流程和方法，而且企业中的每个人明确各自对于数据安全性和完整性所承担的职责。最后，在使用IT工具和实施流程时，上市速度和可接受的风险之间的平衡至关重要。”

Jessica Carroll，美国高尔夫协会信息技术总经理

案例研究

2010年上半年，IBM X-Force研究小组记录了4,396个新漏洞 – 比去年同期增加了36%。报告指出，网络应用漏洞仍是主要的威胁 – 占所有已知漏洞的一半以上。然而，报告指出，企业比以前投入更大的精力去识别和发现安全漏洞。这推动了更开放的协作，可在数字犯罪利用漏洞之前将其识别并予以消除，从而对整个行业产生积极的影响。[1]

沟通方面的挑战

毫无疑问，IT风险管理可创造真正的业务效益。然而，尽管企业可以采用有多种方法发布与风险相关的信息，但沟通仍是切实存在的障碍。据25%的被调查者指出，获得高级领导层的支持仍是一项挑战。30%的被调查者称，他们在向员工传达风险政策和程序方面存在问题。

许多企业采取被动(而非主动)的方式管理和控制IT风险。在很多情况下，信息存在于企业的内部网中，而员工必须花时间搜索这些信息。有些企业将风险管理政策融合到新员工的培训材料中 – 而未考虑将其提供给全体员工的需求。(只有22%的IT经理指出，风险管理政策是每位员工的正式培训的一部分。)也许最让人意想不到的是：不足15%的企业将整合的风险管理计划融合到企业的物理和技术基础设施中。

“我们努力使管理层和职员接受:他们的行为必须不断地修正,以改进安全实践。”

西欧制造业被调查者

“为应对IT风险而获得资金日益困难，即使已经向高管明确传达不应对风险将付出的代价。”

北美洲航空与国防行业被调查者

由于在建立风险意识时可采用多种沟通和教育渠道，因此，企业最好采取更有条理、更详细的方法应对风险，向员工传达这些问题，并且将IT风险管理融合到企业的各个方面。在回答“您的企业主要以何种方式应对风险？”这一问题时，大多数被调查者指出，安全威胁由内部和外部人员(38%)、跨职能高管团队(26%)或指定的风险管理部门(19%)处理。

评估新兴技术

我们向被调查者提出一个问题：他们的企业是否能够获取并部署五种新技术(见图3)：

- 社交网络工具(例如内部网和互联网论坛、即时消息、图书馆、博客和维基等)
- 移动平台(Windows® Mobile、BlackBerry OS和Google Android OS等)
- 云计算
- 虚拟化
- 面向服务的架构(SOA)

在这五种技术中，社交网络、移动平台和云计算的关注度最高。64%的被调查者对社交网络工具风险的担忧程度最高，而移动平台和云计算紧随其后(分别是54%和43%)。大部分风险与数据的访问、使用和控制相关，尤其是对于社交网络，而且与未授权访问机密、专有信息的危险相关。(许多企业尚没有为将社交网络工具整合到基础设施和工作流中而制订流程和方法。)

在我们让被调查者列出与云计算相关的两个最高风险时，大多数人都提到数据保护和隐私(见图4)。业务连续性是半数以上的被调查者考虑的问题，而44%的人认为，私有云比传统IT服务的风险更高，77%的人表示对隐私的担忧。

61%的被调查者认为将数据交给第三方是一种有风险的行为，而只有23%的被调查者担心网络漏洞。仅26%的被调查者指出，虚拟化对企业产生了巨大的风险。与此相似，25%的被调查者认为面向服务的架构(SOA)带来了风险。

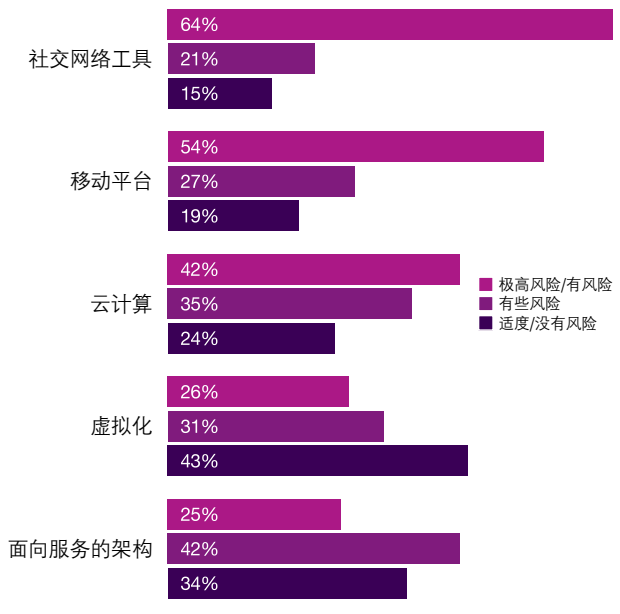

图3. 社交网络、移动平台和云计算是企业最关注的风险

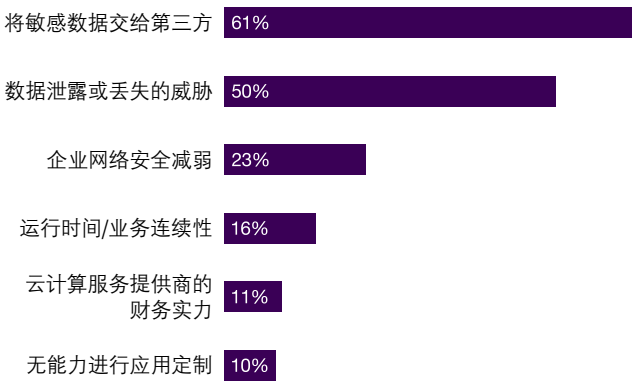

图4. 与云计算相关的风险

信赖云计算

IT经理所面临的压力包括降低与基础架构相关的支出、提高效率和跨业务服务水平等。许多IT经理希望通过云计算帮他们实现这些目标。云计算代表了计算模式的重大进步 – 如同以前的客户机/服务器和大型机计算。工作任务在分布式、全球可访问的IT资源网络中处理，这些IT资源以服务形式按需分配。云计算为IT服务的获取和交付提供了高度自动化、动态的可选方案 – 允许用户将计算资源和服务整合到公共云、私有云和混合云中，而不必直接处理底层的技术。当前，企业纷纷采用云计算的巨大扩展能力和协同能力，以前所未有的新方式解决问题。而且企业正在更快地部署新服务 – 而无需额外的资本投入。然而，企业必须谨慎地选择提供商，尤其是对于与风险相关的问题。

对IT经理的影响

在被调查的IT经理中，大多数被调查者预计他们的职责 – 包括执行政策和程序，为风险控制战略提供意见，帮助制订和/或监督企业的IT风险战略 – 在未来三年内将提高(见图5)。超过65%的被调查者认为，风险控制越来越成为其工作不可分割的一部分，而83%的被调查者认为，IT经理应更多地参与到风险控制活动中。

对于业务与IT的依赖程度日益提高的情况，这些被调查者并未感到奇怪。事实上，被调查的IT经理和CIO认为他们的工作将包括对总体业务战略的支持，以及对企业品牌的支持(例如，在营销和客户服务活动中)。随着越来越多的企业已确定或者“加固”了风险管理战略、流程和程序，对于基础架构的职责可能会转移给供应商或合作伙伴 – 使IT机构将更多精力用于业务安全、弹性和连续性。

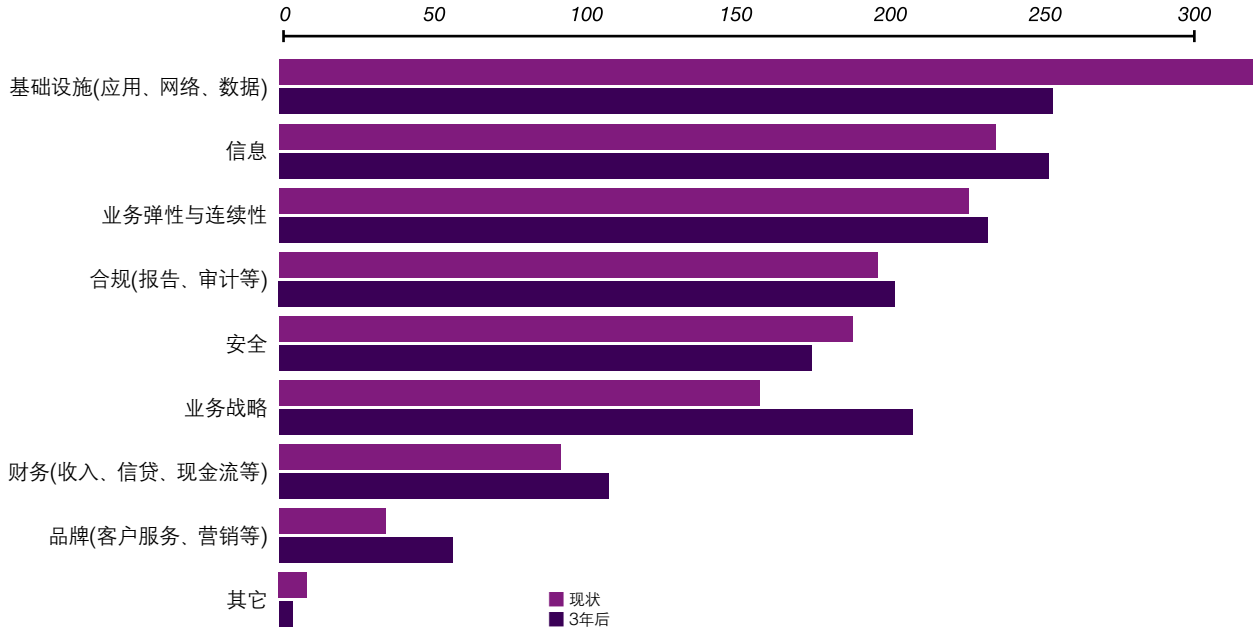

图5. IT经理预计他们的职责领域在未来三年内将发生变化

同样需要指出的是,被调查的131位CEO提供的数据互相参考,对于被调查的IT经理,他们的答案并没有太大差异。

尽管各个行业中的企业已经认识到IT风险管理与合规的重要性，许多企业正在努力改进其业务的这些方面，但几乎没有一家企业为可能出现的所有与风险和合规要求而做好完全的准备。

2010年全球IT风险调研的结果可以帮助IT经理在几个核心方面评估其风险成熟度、确定差距、设定优先次序并制订战略：

- 在企业内，风险意识是每个人的职责。然而，如果与风险相关的政策和程序没有渗透到企业文化中，许多用于管理和控制IT风险的举措可能跟不上，甚至会失败。调研结果证实，企业需要更努力地在企业内教育、沟通和支持风险管理与合规举措。
- 数据是IT风险管理所有方面普遍关心的问题 – 从安全、业务弹性和连续性到可用性、灾难恢复、黑客、合规、基础设施和数据管理。认识到这一点后，企业应以统一的整体方法应对IT风险 – 考虑所有要素，从而为实现更高回报和更高效率的总体目标而努力。

在采用新技术、架构和战略，开发新应用或者集成现有系统时，风险控制应作为一个讨论要点。考虑到积极风险(由于风险伴随着机会，企业主动承担的风险)和消极风险(可损害业务的潜在事故)可创造更多业务价值，并有可能增加收入 – 但只有为IT风险管理提供适当的资金支持才能实现。

并非所有新技术都能带来同样的收益，有些 – 例如虚拟化和云计算 – 可在风险控制的支持和选项方面提供许多好处。尽管云计算要求关注数据安全，但如果部署适当，它可以降低与业务弹性相关的成本，并控制风险。然而，为应对与任何新技术相关的风险而制订流程至关重要。

“如果我们认为知道在何处存在风险，我们有时更愿意单纯地考虑制订一个项目计划，这样，我们就会以此为基础而进行资源分配。”

中东和非洲IT与技术行业被调查者

前景

有效地管理风险是一项由多个方面组成的任务。在处理这项任务时，IT经理应考虑以下方面：

检查并评估企业的IT风险能力

- 为所有风险类别制订跨企业的计划(数据、安全、弹性和灾难恢复，以及新技术)。
- 考虑风险挑战的范围，并确认有既定的计划用于应对每项挑战(按优先次序排列并控制“不利”风险，例如系统故障和安全漏洞)，并确认如何利用“有利”风险(例如加快上市速度和新的客户联系点)。

寻求高层领导的支持

- 成为CIO的可信顾问和宝贵资源；明确表达他们认为应对IT风险的好处。
- “宣传”风险控制的益处，例如更强大的业务增长力量、更高的敏捷性和更有利的品牌认知。

确定如何提高各级以及组织文化本身的风险意识

- 将风险意识融合到日常业务和IT流程中。确保有多种方法用于提高整个企业的意识。
- 制订一个定期传达风险管理范围、合规主题和问题的战略 – 强调这不是“一次性”活动。

寻找创新的方式实施风险控制程序

- 将与风险相关的程序结合到IT基础架构中，而不是孤立地将其结合到应用中。
- 检查业务流程，以确定潜在风险问题，并制订可在整个企业内执行的特定IT风险治理计划。

确保拥有防护措施，帮助预防在未授权情况下访问企业数据和系统

- 审查业务连续性计划。业务连续性不仅包括自然灾害计划；而是包括全面的业务中断场景 – 从服务器故障到全面瘫痪。
- 使每个人了解自己对于保证数据安全和受保护的职责 – 以及如何履行自己的职责。
- 确定保证数据安全和受保护的工具、流程和方法论。需要注意的是，许多已经存在(身份接入与控制；主数据管理；信息生命周期管理；数据所有制流程)。

新技术是否应引入到企业中已经不再是一个问题，而真正的问题是何时引入。如前文所述，并非所有新技术都能带来同样的收益，有些可在IT风险管理方面提供巨大的好处。虚拟化和虚拟机等新技术为控制风险和降低成本提供了优秀的方案。

强有力、循环的IT风险治理 – 从技术和业务角度讲 – 由于持续地评估业务对IT风险的脆弱性，确定这些风险的优先级，并应对这些风险。因此，将风险管理协议整合到实施的新技术中非常重要。

最后，在实施工具和流程时要考虑业务的需求。平衡上市速度和可接受的风险。通过主动地进行IT风险管理，企业能够及早地消除漏洞，并且在出现计划内或计划外的事故时保持安全和弹性。

您是否做好准备?

- 您的企业是否评估了风险成熟度并管理风险，包括业务以及IT基础架构和资产方面?
- 您的企业制订了哪些战略,以遵循行业和IT领域关于控制风险的最佳实践 – 从安全开始,并包括弹性和业务连续性?
- 在您的企业中，与风险相关的举措如何帮助提高洞察力和控制能力，并帮助确保对合同、行业标准、法规和内部控制措施的遵循?
- 您的IT基础架构如何在灵活性、安全性、可用性、治理、扩展性、弹性等方面支持持续的业务绩效目标?
- 您的企业制订了哪类计划，用于确保人力资本、流程和系统能够恢复并应对中断事件?

要访问更多的IT风险管理资源，请访问：
ibm.com/smarterplanet/security

关于作者

Linda Ban，BM商业价值研究院的CxO调研计划主管和应用创新服务(AIS)负责人。Linda的丰富背景包括在新兴技术和协同技术、业务和运作战略、系统开发以及运作管理方面的丰富经验。除了与客户合作外，她还发表了关于多种业务主题、挑战和解决方案的文章。
Linda的联系方式是：*lban@us.ibm.com*

Richard Cocchiara，BM杰出工程师和IBM全球企业咨询服务部的业务连续性与弹性服务首席技术官。他拥有28年的I/S经验，并且为多家财富500强企业开展了咨询项目，尤其是在金融和证券行业。
Richard的联系方式是：*rmcocch@us.ibm.com*

Kristin Lovejoy，负责IBM安全战略的副总裁。她拥有关于面向对象的风险管理模型和方法论的美国和欧盟专利。
Kristin的联系方式是：*klovejoy@us.ibm.com*

Ric Telford，IBM云服务的副总裁，他的职责是定义IBM全面的云计算产品的新机遇和服务。Ric的联系方式是：*rtelford@us.ibm.com*

Mark Ernest，IBM杰出工程师，并且是IBM技术研究院的成员。
Mark的联系方式是：*lernest@us.ibm.com*

选对合作伙伴，驾驭多变的世界

IBM全球企业咨询服务部积极与客户协作，为客户提供持续的业务洞察、先进的调研方法和技术，帮助他们在瞬息万变的商业环境中获得竞争优势。从整合方法、业务设计到执行，我们帮助客户化战略为行动。凭借我们在17个行业中的专业知识和在170多个国家开展业务的全球能力，我们能够帮助客户预测变革并抓住市场机遇实现盈利。

参考资料

1 The IBM X-Force 2010 Mid-Year Trend and Risk Report. IBM Corporation, 2010.

北京总公司

北京朝阳区北四环中路27号
盘古大观写字楼25层
邮编：100101
电话：(010)63618888
传真：(010)63618555

上海分公司

上海浦东新区张江高科技园区
科苑路399号10号楼6-10层
邮政编码：201203
电话：(021)60922288
传真：(021)60922277

广州分公司

广州林和西路161号
中泰国际广场B塔40楼
邮政编码：510620
电话：(020)85113828
传真：(020)87550182

GBE03365-CNZH-00