企业风险管理教程

企业风险管理教程

企业风险管理（ERM，enterprise risk management）的目的是使一个组织的资产及所得所受的风险影响减为最小。如今，云计算等技术改变了企业应用信息系统、以及如何达到安全风险管理和合规遵从的方式，企业需要重新计划并部署自己的风险管理。那么究竟该如何制定安全风险管理计划？又有哪些风险管理的最佳实践可供企业参考？本技术手册将分三部分为你详细介绍企业风险管理，包括企业风险管理的概念，风险管理的实施及最佳实践。

企业风险管理的概念

企业风险管理（ERM，enterprise risk management）是一个计划、组织、领导、控制一个组织的活动的过程，其目的是为了使一个组织的资产及所得所受的风险影响减为最小。企业风险管理的过程不仅涉及与意外损失相关的风险，还扩展到财政、策略、运营及其他风险。

- ❖CIO 新词解：企业风险管理
- ❖准备迎接风险管理挑战
- ❖创建规则遵从文化　促进信息安全合规管理和风险管理

风险管理的实施及解决方案

IT 风险管理正处于十字路口。有超过 2000 名美国受访者参加了最近的一次 IT 专业人士 ISACA 调查，据调查报告显示，改善经营业绩是驱动他们所在组织 IT 风险管理的主要动力。企业在制定安全风险管理计划时，应该参考什么资料？具体步骤是什么？

- 如何制定安全风险管理计划
- 业务合作伙伴安全：管理业务风险
- 五个步骤：从 IT 风险管理到业务风险管理
- 2011 年最佳策略及风险管理产品

几大风险管理的最佳实践

不同规模的企业都面临着多方面的严重威胁，这包括来自电邮、Web、即时通信、雇员等。这些威胁的复杂性、速度和变化都在以无法预料的步伐不断发展。更糟的是，多数企业感到，它们缺乏能够正确解决这些现代威胁的资源。本部分将介绍几大企业风险管理实践，让企业从一个风险管理的 “挣扎者”，变成最佳的信息安全“X 战警”。

- 应用开发外包风险管理
- 备份质量对风险管理策略至关重要
- 七大最佳实践打造信息技术风险管理“X 战警”
- 供应链风险管理最佳实践及业务连续性

CIO 新词解：企业风险管理

企业风险管理（ERM，enterprise risk management）是一个计划、组织、领导、控制一个组织的活动的过程，其目的是为了使一个组织的资产及所得所受的风险影响减为最小。企业风险管理的过程不仅涉及与意外损失相关的风险，还扩展到财政、策略、运营及其他风险。

近年来，各种组织已将外部因素列为 ERM 中越来越重要的影响因素。行业及政府的管理机构，还有投资者，已经开始细察公司风险管理的政策及过程。越来越多行业都要求董事会检查报告他们所管理的组织的风险管理过程的足够性。

金融机构兴旺于风险商业，他们就是得益于有效的 ERM 的最好例子。他们的成功取决于很好的处理了增加利润和风险管理二者间的关系。

商业风险管理（Business risk management）、全面风险管理（holistic risk management）、以及策略风险管理（strategic risk management）是同义词。

（来源：TechTarget 中国）

准备迎接风险管理挑战

云计算改变了企业应用信息系统、以及如何达到安全风险管理和合规遵从的方式。

当信息安全规划经理辨认那些会影响企业安全策略的关键主题时，云计算无可争议地从中脱颖而出。

困难的经济环境确实有助于让云计算变得更有说服性。因为按需的资源是动态可扩展的和灵活的，这对于大型和小型的企业来说极具吸引力，且无疑会继续改变我们应用信息系统的方式。

对于每个努力保护组织的网络用户和数据的人来说，迁移到云计算会引起巨大的变化和挑战。合规要求最有可能会妨碍企业迁移它所有的数据和操作到云上，所以，事实上这个转变是额外的安全挑战，位于保护现有的网络基础设施之上。迁移到云上，要求数据和应用放置在已完善建有边界防御和物理访问控制的区域之外。随着不受到 HR 控制的用户数量的增加，如供应商、客户和合作伙伴，都会通过基于 Web 的协作工具来访问你的数据。IT 管理员已经疲于确保访问公司网络的移动用户的安全，而云计算又是一个完全不同的规模。

对于我来说，关键的安全挑战之一，是如何对位于企业防火墙之外的员工、客户和合作伙伴进行有效地管理和执行访问控制。云计算把我们都变成远程的工作者，且按定义来说，云应用和数据都位于企业之外。这意味这你不能再依赖多层认证、防火墙和其它边界防护来为你完成工作。

从战略角度来看，管理这些挑战需要很多行动。必须评审和加强 HR 的安全策略以便他们来执行健全的用户管理生命周期。详细的身份和访问管理策略也必须到位，一个能充分利用联合的身份管理，一个能让用户跨自治的安全域安全地访问数据或系统的安排。我建议在你的企业应用内启用单点登录（SSO），并利用这个架构来简化云提供商服务的集成和实施。

云计算同样要求更加可靠的因特网连接，所以即使是微小的操作也会需要建立某种形式的冗余性，来确保数据和应用一直都可用。无论如何炒作，云服务仍然是十分不成熟的，有一些或其它形式的运行中断状况发生。有些可能很容易破产，它是一个处于脆弱的经济环境中的新兴行业。多个服务提供商会提供你更好的网络多样性和业务连续性，所以任何基于云的项目应该采用厂商中立的应用和数据架构。这包括以独立于云方式的备份，和一个独立的机器镜像。你需要尽可能地让这个转变是简单的，或者有应变计划可以将操作回撤到内部运行的云环境。

尽管云计算可能会减少一定的连续性问题，但它永远不会消除行之有效的业务连续性计划的需要。

在不久的将来，基于云的服务和云计算技术会经历激增且长时期的攻击，因为对于黑客和网络恐怖分子来说，它们是具有吸引力的目标。因此，建立一个数据加密策略并实施技术来支持它，是最佳的主动防护措施。被加密的数据本质上是受到保护的，这也是为什么这么多法律和合规强制实行这个实践。加密也允许你区分角色和数据，当加密密钥控制访问你的数据时。

不断地，你会看到很多新的基于云的服务上线，许多为企业带来了可观的经济回报。一些无疑会改变长期建立的风险与回报关系。而且当评估转变为基于云服务的投资回报率（ROI）时，你会需要评审组织的业务策略和对于风险的态度。云计算正在改变信息系统，所以要确认考虑到，如何在任何新的业务流程中融入安全，从而使基础设施、数据和用户继续受到防护。

三个主要的风险管理挑战

1. 尽管云计算可能支配 IT 策略向前发展，安全经理还是需要关注其它领域。当然，和云计算紧密相连的是虚拟化技术。这个行业仍然奋力为虚拟化环境定义安全最佳实践，因为应用和数据从单独的服务器迁移到在线的网络上。跟踪事态发展在安全控制方面的发展是重要的，以及对这些系统的威胁。

2. 智能手机是网络环境外安全经理仍在致力于完全控制的另一方面，我们开始看到对移动设备有效的攻击，并且它们会变得更加流行。不会消耗完电池或 CPU 的安全软件会成为必不可少的部分。

3. 最后随着 VoIP 使用的增长，有组织的罪犯们会发起许多攻击。系统管理员需要更加关注 VoIP 隧道的安全，使用加密而不是修补服务的质量。

是的，安全是一份永远不会结束的工作。

（作者：Michael Cobb 译者：Odyssey 来源：TechTarget 中国）

创建规则遵从文化　促进信息安全合规管理和风险管理

很多时候，在考虑建立或者扩大信息安全性并报告给高级管理层时，我们面临的最大挑战不是技术上的，而是文化上的。

业务经理犹豫是否应该突出有风险的领域，因为他们担心会被人认为没有尽忠职守。律师担心在文件中出现漏洞，因为某些漏洞最终会对组织不利。有时，经理们不愿意对公司高层讲的太多，虽然其中确实可能存在很大的风险，但是他们担心高层不能完全理解这些信息，只会再提出一些无理的要求。

这就是我们作为安全和规则遵从管理人员所面临的现状。如果成熟的公司想全局把握信息安全的风险和规则遵从，这些问题都是必须首先要解决的。

与许多人所认为的相反，在寻求解决安全和规则遵从的弱点时，知识就是力量，且保持良好的透明度是一件好事。不过，要成功的跨越文化障碍，从而有效地报告信息安全状况，是需要策略的。一些经过时间考验的解决方案，它们可以用来解决这些阻碍有效管理信息安全风险及规则遵从的文化障碍。

培养规则遵从文化的几个建议：

使用直白的语言——毫无疑问，在信息安全报告中决定成败的最重要因素是语言。简单地说，任何报告（无论是在记分卡或叙述）必须只限制使用基本的业务术语。不要使用 IT 术语，不使用任何模糊的缩写，不要出现特例。一个 IDS 系统或其他网关设备可能有一份很好的 20 页的详细技术报告，虽然可能对技术人员有帮助，但它们不应该出现在提供给高管们阅读的报告中。相反，应该要求写这些报告的人去总结这些数据，使用尽可能简洁的语言，以便让不熟悉该项技术的人也能理解。

公开是安全的——第二大重要的因素是营造一种环境，让人在这种环境下意识到公开是安全的。这意味着人们被允许表达他们所观察到的潜在危险和操作失败而不会受到惩罚，管理人员应该在条件允许时营造这样的环境。对于观察到的风险，重点必须放在风险评估及应对方案分析。对于操作失败，报告重点应放在 1)发生了什么事情，2)应该对其做什么，3)怎么样使它不再发生。责怪是合作的死敌，因此任何纪律处分，必须私下进行。一旦人们开始意识到风险和失败都可以提出来进行合理、健康的讨论时，越来越多的风险就会突然被人们注意到。

重点放在解决方法上——简单地说，要确保向管理层汇报任何重大的风险，应该包括了对该风险有一个管理层水平的评估和一个行动计划（或至少提供一些选项）。过分强调风险本身并不能解决问题，还经常给人没有做好份内工作的感觉。但是，提出风险的同时顺带一系列的解决方案，会强化一个事实：这个人有在做事。

让他们做决定——当提供关于信息安全计划的遵从规则的内容时，除了让管理层了解情况，还应该给予他们做决定的机会。即使这意味着对于某一关注的领域只是简单地提供了一些选择，这也利于让他们参与进来，并引起重视。这看上去存在风险（试想谁真的指望“秃头老板”能做出实质性的决定？），但是当风险被解释清楚、选择范围也明确时，老板们也愿意参与进来。 相信我，参与真的是一件很好的事。

从小事做起——事实上，很多企业无法从零一步建立很详细的计分卡，这也从未发生过。从小事做起是专注更多的可以使管理人员采取行动的无害基准点（data point）（如，培训结束，第三方管理等）。随着管理层逐渐熟悉报告的模式和周期，他们会把注意点转移到更敏感的话题，比如公开审计问题、控制失误、操作事故和风险热图（heat map）等（后者更直接的和具体业务领域相关）。

最后，我们的目标是通过对话和接触来建立一个规则遵从文化。从小事做起，保持格外清晰，保持紧迫。最终，人们会发现这些建议比想象中的友善，进而会进行反思，并建立论坛用来讨论一系列对公司有益的问题，最终建立起可以更好为企业服务的规则遵从文化。

（作者：Eric Holmquist 译者：Sean 来源：TechTarget 中国）

如何制定安全风险管理计划

问：我们公司第一次制定正式的安全风险管理计划，您能提供一些安全风险管理计划示例吗，或者就安全风险管理计划应包括哪些内容给我们提供一些建议吗？

答：在制定企业安全风险管理计划时，有许多资料可供参考。第一份应该参考的文档是NIST（美国国家标准与技术研究所）特别出版物 800-53 V3——《美国联邦信息系统和组织安全控制建议（Recommended Security Controls for Federal Information Systems and Organizations）》。该标准的第三章给出了一个规范的流程图（如图 1 所示），可以为你们制定安全风险管理计划和框架的关键流程提供有益的指导。

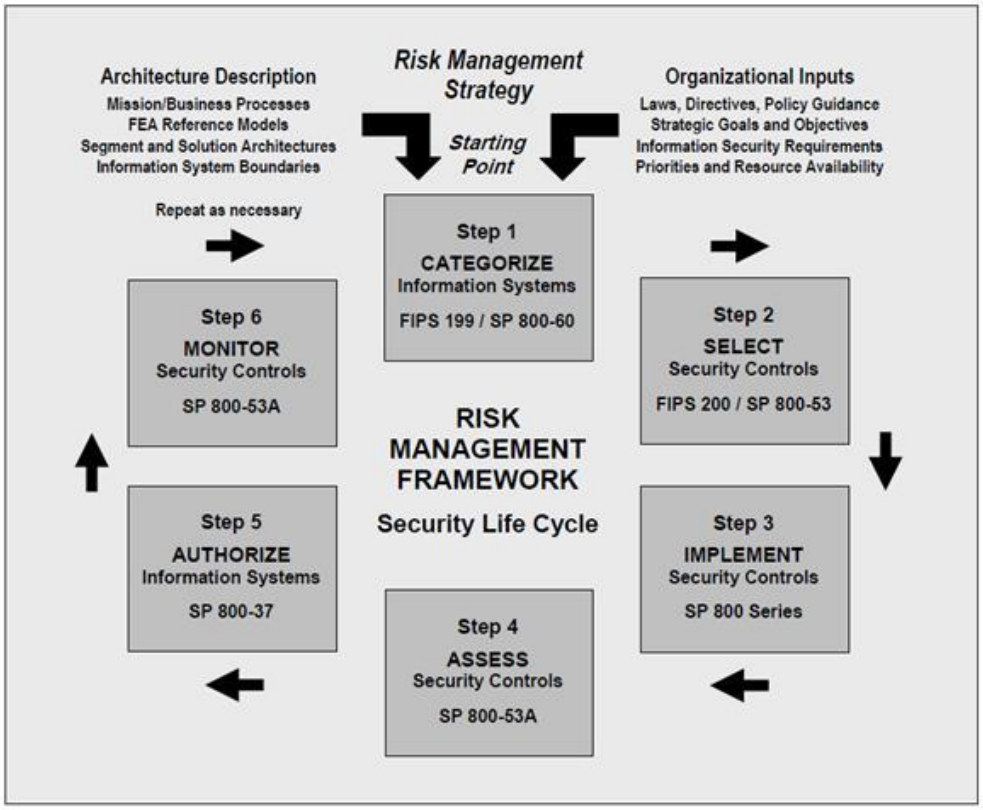


FIGURE 3-1: RISK MANAGEMENT FRAMEWORK

图 1

从本质上讲，制定安全风险管理计划的出发点是将“组织投入”和“体系结构描述”作为基本信息，帮助企业进行资产识别和分类。

例如，组织投入可能包括组织不应受到妨碍的核心业务、企业的主要客户以及企业必须遵守的主要适用法律等。

体系结构描述包括企业使命/业务流程、系统体系结构以及需要保护的信息系统的边界。

另一份值得参考的文档是 NIST 特别出版物 SP 800-39——《信息系统风险管理草案（DRAFT Managing Risk from Information Systems）》，该文档提供了在信息系统和基础设施中实行安全控制的组织的风险管理常规视图。该文档还提供了一个风险管理的高层次视图，如图 2 所示。

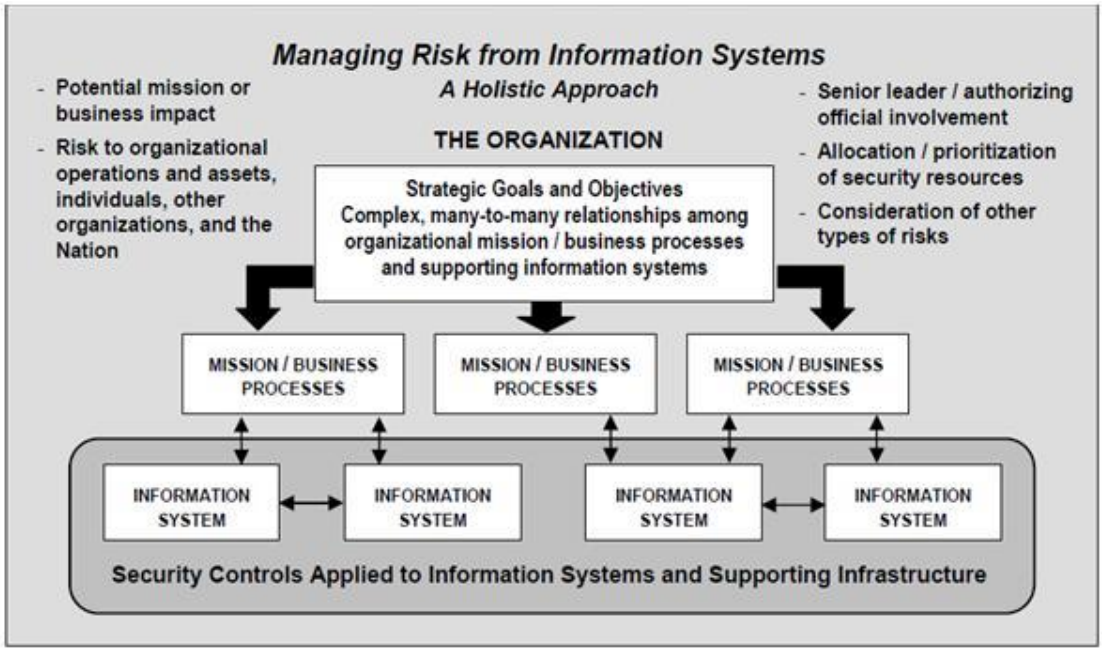


FIGURE 1: ORGANIZATIONAL VIEW OF RISK MANAGEMENT

图 2

对制定风险管理计划可能有所帮助的第三份文档是《信息安全（Information Security）》杂志 2009 年 6 月发表的一篇开创性的文章——《如何制定融合业务和安全需求的风险管理方案（How to write a risk methodology that blends business, security needs）》，其作者是我的同事 Cris Ewell。Cris 在这篇文章中指出，制定风险管理计划和流程时应注意以下要点：

“风险管理流程必须植根于安全性原则并与安全计划整合，安全计划包括业务需求、合理注意事项、当前攻击向量以及符合法规要求和合同要求。遵守标准和法规的要求有助于表明合理注意，但不应成为安全计划的推动力。风险管理不可能解决所有的威胁和脆弱性。在一个组织中，信息安全实践的发展方向、评估指标和改进方法的推动力应该是降低剩余风险，而不是实行指令性控制。”

在这篇文章中，Cris 还从战略、战术和业务三个方面介绍了如何构建风险管理框架，共涉及下列 13 个安全要素：

- 战略类

1. 组织和授权

- 战术类

1. 策略
2. 审计与合规性
3. 风险管理
4. 隐私
5. 突发事件管理
6. 教育和培训

- 业务类

2. 业务管理
3. 技术安全和访问控制
4. 监视、测量和报告
5. 物理和环境安全
6. 资产识别和分类
7. 帐户管理和外包

你可能还想从互联网上查找其他的风险管理计划资料。不过，需要指出的是，前面提到的 NIST 文档和 Cris 的论文都是优秀的资源，而且可以免费获得。

（作者：Ernest Hayden　译者：王勇　来源：TechTarget 中国）

业务合作伙伴安全：管理业务风险

在发明计算机前，围绕业务合作伙伴的安全问题就已经是现实。为便于讨论，业务合作伙伴是指和你的企业有业务关系的个人或组织，并且作为合作关系条款中的内容，他们能够访问一些敏感数据或系统。

当组织和业务合作伙伴互相联系并且为对方提供对内部系统更多的访问时，更多的信息安全挑战就产生了。因为业务合作伙伴通常与受信任的内部人员或外包商一样，拥有相同的数据或系统访问级别，组织承受着许多显著的信息安全挑战，这与组织已经面对的内部威胁风险相似。业务合作伙伴的特权访问只是放大了风险，像任何内部人员一样、业务合作伙伴能够绕过为阻挠外部或非信任源访问而设置的安全控制。

组组织需要进行尽职调查，以确保其免受于业务合作伙伴所带来的风险。本文中，我们探讨涉及到业务合作伙伴的典型风险以及缓解这些风险的方法。

涉及业务合作伙伴的典型风险

涉及到业务合作伙伴的典型风险主要依赖于访问的类型、数据和可供访问资源的风险级别。业务合作伙伴能以许多不同的方式访问内部的网络：直接的物理访问、本地或远程的凭证登录。从业务流程的角度来看，这样的访问对于业务合作伙伴扮演的角色是关键的，但是从安全的角度来看，这种情况是设想合作伙伴知道如何并且负责地使用该访问权限。不过，现实情况不总是这样的。

类似地，另一个风险是，与你的组织相比，业务合作伙伴实行的信息安全实践不太安全。在一些合作伙伴组织中，共享个人的登录凭证就像常规一样，这可能导致伙伴的访问权限被窃取或是无意地被用来攻击你的系统。通常这种使用合法的访问凭证、通过受信任的连接进入的攻击手法很难侦测。例如，如果业务合作伙伴的系统设定为能通过 SSH 经由因特网远程访问他们的网络，一旦他们使用的单因素认证和密码被恶意软件捕获或是被暴力破解，攻击者就可以使用这个账户通过受信任的网络连接攻击你的系统。在业务合作伙伴的网络到你的组织间使用受信任网络连接，使得该攻击难以侦测，因为它可能不会通过你的边界安全检测。

另外，业务合作伙伴可能访问、存储或处理数据的风险，会因业务合作伙伴关系的不同而不同，但是比起访问系统来说，这可能会有更大的风险。如果业务合作伙伴存储像社会保险号这样的敏感数据，并且他们的安全防线被突破，你的组织可能需要负责把这个安全事故、相关

的成本和潜在的责任告知你的顾客，即使你的安全没有直接地受到损害。对于合作关系来说，更严重的风险是与业务合作伙伴共享的知识产权遭受任何未授权的访问。

缓解和管理业务风险的方法

总之，管理与业务合作伙伴安全有关风险的最佳方法是，实施强大的安全控制。你的组织能够实施以下这些技术，来确保业务合作伙伴对你组织系统访问的安全：对所有的数据传输使用加密的连接，要求所有的访问通过使用强认证个人帐户，记录所有的访问和活动，然后审阅这些日志来寻找可疑的活动。合适的业务控制包括对新用户的正确授权，由管理层审阅访问列表以及合同中定义合作的关系。

与业务合作伙伴的合同应该包括对安全控制的引用，包括希望伙伴满足的职责和期望，例如员工必须遵守一样的安全策略。该合同应该包括关于报告安全事故、保护系统和数据所需提供的最少的安全控制的细节，以及访问方面的细节。包含以上条款的合同，或是对已存在合同的内容补充，会有助于确保对双方的期望得到理解。

对于那些不寻常、或是涉及到安全团队认为可能带来更高安全风险的业务合作伙伴安排，你的组织可以进行风险评估，这是在执行合作关系前应努力一部分。这可以确保管理层和其他利益相关人理解赋予业务合作伙伴访问你们系统所涉及到的技术风险，本质上，这是让管理层推进合作关系的决策，（对合作伙伴）进行专门的控制来降低风险，或是选择不发起业务合作。

管理业务合作伙伴或是受信任内部人员的风险另外的方法是，记录并定期审查日志，从而寻找可疑的行为。根据日志的数量，这可能需要自动的工具来帮助辨识需要人工调查的事件，但理想情况是，你的安全团队已经有合适的日志审查能力来做这个事情。

一开始，如果你实施强大的安全控制、进行风险评估或是定期地审阅相关日志，会让你的业务合作伙伴觉得你不信任他们。如果对于所有的业务合作伙伴遵循一样的实践和评估模型，就会很容易让潜在的业务合作伙伴将那些作为标准，从而尽职尽责。同样你要谨记，如果你没有遵守对业务合作伙伴提出的安全需求，业务合作伙伴可能会对提供你的组织到它们系统的任何访问感到担心，并使两者间的关系变得紧张。

管理业务合作伙伴风险：结论

毋庸置疑，在当今以计算机为中心的世界中，为快速地和有效地进行业务，新的业务交互和赋予业务合作伙伴访问权限已经引起了新的风险。对系统和数据新增的访问权限给组织增加了风险点，但是围绕业务合作伙伴的这些安全风险是可以成功缓解的。记住，尽管业务合作伙

伴安全风险总会以某种形式存在，但最终安全的角色是为业务领导者提供建议，关于这些风险、以及如何控制到位从而最大程度地缓解这些风险。

(作者：Nick Lewis 译者：Odyssey 来源：TechTarget 中国)

五个步骤：从 IT 风险管理到业务风险管理

IT 风险管理正处于十字路口。有超过 2000 名美国受访者参加了最近的一次 IT 专业人士 ISACA 调查，据调查报告显示，改善经营业绩是驱动他们所在组织 IT 风险管理的主要动力。在印度和澳大利亚/新西兰的类似调查报告也发现，驱动力从法规遵从转向了经营业绩。通过比较可以看到，法规遵从被认为是风险管理的首要驱动力，占受访人群的 20%到 28%，不同的国家比例略有不同。

对于 IT 风险管理者来说，这是一个绝好的机会，他们可以证明 IT 对业务有更多的影响，尤其是在经济危机影响压力较大的国家。

要利用好这个机会，主动的 IT 风险管理者可以采取下面五个步骤：

1. **从业务方面开始。**要带来业绩方面的益处，需要在 IT 风险方面投入精力，因为它们与业务目标密切相关。

2. **定义风险评估范围。**要针对给客户提供服务的业务活动建立框架，而不是针对技术。

3. **寻找愿景。**对业务资产和资源的威胁，从更宽泛的范围来看待。

4. **使你的工作更容易。**广泛利用已经采纳的方法和技术来评估和应对风险。不要重新发明轮子。

5. **把要做的事说清楚。**如果你对业务进行关注，请一定让业务领导搞清楚。要使用业务的语言清楚地表达你的计划和成就。

面对新法律和法规的大肆鼓吹，企业部门命名都显得与“合规和风险”有关，这样的调查结果多少有点出人意料。与合规遵守方面的压力一样大，企业领导会紧紧抓住机会，而不是在经营业绩背后强调 IT 风险管理。从华尔街的报告中可以很清楚地看到，削减成本的盈利方式并没有满足投资者期待的收入增长。标准普尔 500 指数从年初至今基本持平。此外，成本削减增加了自身风险。

要实施第一步，CEO 和关注收入增长的首席财务官（CFO）为 IT 风险管理者变成为 IT 业务风险管理者提供了一个起步点。请为你的企业（跟你的角色有关，也可能是部门）评估业务

绩效报告和当前 IT 风险报告。要看看从业务绩效度量到 IT 业务风险存在明确的联系吗？业绩度量包括销量，客户满意度，产品发布时间以及诸如扩张、收购和兼并等策略的成功。

对于业务线，职能部门和区域主管也有度量，他们被据此评估并支付奖金。要把这些实实在在的措施映射成 IT 必须做的事情，来支持他们。然后确定对于业绩与 IT 相关的风险。例如，市场份额增长可能依赖于新的销售和支持渠道。这可能依赖于移动客户服务应用程序，它依赖于整个 IT 堆栈。

第二步的基础是由 IT 绩效经营业务目标的这种依赖分析和 IT 对业绩的相关风险提供的。什么样的风险评估范围可以给你更多帮助呢？应该从诸如网络或者数据存储这类技术角度构建风险框架吗？或者，是不是面向针对市场份额增长策略建立风险框架更强大呢？因为你可以向首席营销官，CFO 以及其他高度关注业务成功的人展示成果。

第三步涉及检查对业务资产范围（包括 IT 堆栈）的更广范围的威胁，用来提交风险评估范围的商业利益。对于 IT 风险管理者来说，这可能是最困难的转换，这些管理者是从管理 IT 竖井中的风险（比如：项目管理、安全、恢复或者变更管理）中提升而来。现状，管理者必须评估来自各方面的威胁，包括自然的，恶意的，意外发生的，以及业务量来源的威胁；要针对真个 IT 堆栈进行考虑，包括：应用程序、中间件、服务器、数据、存储、网络、设施以及 IT 管理流程和软件工具。

第四步：使你的生活更轻松。有太多的企业都在重新发明轮子，建立他们自己的风险管理框架来定义一组合规要求。当这些合规需求发生变化时，风险框架中的硬编码也需要相应改变。此外，对于每个 IT 竖井，对于整个 IT 风险的伞状管理，组织可以利用由专业组织和标准制定机构提供的一些开放的业界实践和指导。这些工作最好是基于同行评审进行，并经常更新，还要培训和建立活跃的用户社区。

最后，要奖励在“身体力行”经营业绩之路中所有良好的表现，记得要与业务方面“交流”。当你寻求业务案例来支持和报告结果时，你应该就业务目标的实现加上评论内容，这是与第一步相对应的。同样的对应关系现在可以使主管们更容易理解“这对于我意味着什么”，同时认识到你的努力如何给他们带来了收入增长。

（作者：Brian Barnier　译者：冯昀晖　来源：TechTarget 中国）

2011年最佳策略及风险管理产品

金牌获得者

McAfee ePolicy Orchestrator（迈克菲系统防护解决方案，简称ePO）（迈克菲）

读者将策略及风险管理的金牌颁发给迈克菲公司的ePO产品，特别引人注目的是该产品在辨别安全风险和策略违规、策略管理、报告及告警和易于安装方面的能力。读者还喜欢该厂商的服务和支持，以及它带来的投资回报率。

作为迈克菲安全管理平台的基石、迈克菲的ePO产品统一了安全管理，允许客户将行业领先的安全解决方案引入他们的企业基础架构设施，以便加强可视性、获得效率并提高防护水平。

该产品提供了端到端的可视性，包括能够拖放的仪表盘，它提供跨终端、数据、手机和网络的安全智能，以及可以将迈克菲和第三方安全解决方案与客户的LDAP、IT运维和配置管理工具连接起来的开放架构。该产品还简化了安全操作，允许客户将管理的任务流水化、缓解审计的繁琐工作，减少安全管理相关的硬件费用。

“策略和风险管理与企业的许多方面戚戚相关，所以即使在缺少像萨班斯法案这样的单个外界压力下，这些产品仍然有广泛的采用空间。新的竞争者不断地进入这个市场，这个市场的产品一直在变得更加成熟”。——Forrester Research公司的高级分析师Christopher McClean

银牌获得者

Tripwire Enterprise软件（Tripwire）

铜牌获得者

RSA Archer eGRC Platform（RSA的Archer eGRC平台）

EMC安全事业部RSA

（作者：Information Security职员　译者：Odyssey　来源：TechTarget中国）

应用开发外包风险管理

随着协作和远程访问技术的发展，在和应用开发外包伙伴协同工作中暴露出来的问题部分地得到了解决，但是，在代码外包甚至离岸的的过程中，仍然蕴含着大量的风险。

比如说，我们访问一个技术博客，很可能会发现这样的帖子，某位应用开发人员正向其他人详细的讲述其最新接手的财富 500 强公司的项目，于是乎问题随之而来，这位开发人员很可能将那家 500 强公司的应用开发的敏感信息展示给了全世界。

“情况一直如此，”Tim Vibbert 如是说。Vibbert 是某大型外包商的前任企业架构师，也曾经在一些大公司任内部架构师。Vibbert 现在南新泽西管理着一家名为 Oglala Innovative Solutions 的咨询公司，他说：“在某项目的开发过程中或者之后，开发人员在博客上发布的文章，导致了整个项目的知识产权泄密。直接后果就是竞争对手使用这些免费获得的信息作为自己的开发模版”。

Vibbert 说为了把这种应用开发外包过程中的风险降到最低，越来越多的公司将更加严格的条款写进外包工作声明中，这些条款涉及了项目的开发人员可以分享项目信息的方式。Vibbert 说：“由于博客这种媒介形态的出现，各个公司正在以合同的形式对项目细节讨论的方式和位置作出限制。”

与此同时，各公司也要求其首要的外包伙伴负责在子承包商之间加强这种交流限制。这就引出了另外一种日益受到关注的外包风险：到底是谁真正承接了项目？Vibbert 说：“当你和一家大的外包商合作时，你的项目可能会被分块转包给各种专业的公司，所以你要确保你了解这种情况。”

谁负责我的代码开发？

作为一位前项目经理，Mary Gerush 将会告诉你在和外包供应商合作的时候，选择和保持应用开发人员的选择非常困难。和供应商建立长期的关系会很有帮助，但是即使是你自己选择的开发人员也通常会扔下你的项目去做另一项。

Gerush 在印度外包项目的方法是了解扩充的团队中的每个人。“过一段时间，你就知道税收最好的开发员，这样你可以和他们建立稳定的关系，并建立忠诚度。” Gerush 是 Forrest 的分析师。

有一位 CIO 最近被公司的管理团队问到，当公司在子办公室聘用了开发人员的时候，为什么还要绕很多安全的圈子在公司的外包合作商那里聘用同一个国家的开发人员。

Forrester 的分析师 Khalid Kark 说，这家公司在俄国，而俄国没有等同的背景核查。“那位 CIO 说‘我们对（我们国家）自己的员工都作了背景核查，我们了解我们（应用开发员）的情况。’”

这位 CIO 并不太确定，但是外包供应商也有同样的规则，以确保进来和出去的是谁，他们可能带着敏感信息。

建立控制来管理应用开发外包风险

很多企业在事后学到的一个教训是当应用开发外包项目已经在进行的时候，设置安全控制就困难对了。有些专家还会把外包商做的应用开发不经过前期的应用开发工作测试或监控，就放入他们自己的环境。在这两种情况中，安全都向市场的速度作了倾斜。

Kark 说：“应用开发团队没有安全技术，这样公司就必须成立一个安全团队，在应用开发进入他们的环境前和在开发过程中监控和测试应用开发，这样也会延缓工作进展。”

几年前，和外包商的应用开发合同中大约有 5% 到 10%中包含 了详细的严格的安全策略和控制要求。KarK 解释说，现在随着公司把更多的责任交给外包商，这个比例已经上升到 30%到 40%。

企业不但要求内部使用和访问控制相关的策略同一等级的控制，而企业他们还想要了解外包商是否具备 ISO 27001 或者 ISO 27002 证书。他说，他们经常把在线访问写入合同，测试外包商的安全监控工具和策略。

Kark 说：“他们要了解谁访问了、怎么访问的、是否做了背景核查。如果他们看到这些策略没有执行，他们就会认为这是合同的泄漏。”

通过设置期望和阶段性目标管理风险

Vibbert 曾经做过一个项目，应用完成了，所有的代码也一起出来了。一起出来的还有巨额帐单。

他说：“公司可能会拿到一份巨额帐单，而且没有办法验证，然后就可能涉及法律，那么这家公司就非常不走运乐，因为他们没有设置详细的交付产品或者交付产品的成本。”

最位一位项目经理，Vibbert 会设置和产品发布一样的交付——本周是第一个版本，下周是第二个版本，以此类推。“我们提前说好，并写下来，10%的工作必须依照某些详细的规定在某个可以继续前进的日期做完。”

以下是企业可以在管理应用开发外包风险的时候采用的预设步骤：

- 提前检查应用开发设计，不只要设定交付的产品，还要确定完成项目需要的技术范围。

- 确定开发人员不会偏离设计标准。如果应用可以以某种方式用 Java 编写，确保外包商的开发人员都遵守这个计划。

Vibbert 说：“你看到的是开发人员认为他们知道更好的方式，这样他们就会用自己的方式做，然后公司拿回来了代码，而自己的开发人员不知道该怎么办。”

- 建立一个团队监控外包商的状况和所在的国家。一个厂商管理团队应用可以找到这个国家发出的任何声明，例如可能的收购，还有外包商所在国家发生的可能中断项目的政治冲突。

Gerush 说：“厂商管理办公室应该警惕任何问题，并制定风险出现的计划，这样公司公司就不会被动确定海外的数据会发生什么了。”

- 不要忽视一个国家的隐私法律。例如，中国对进出国界的数据都要监察。“一个国家可能聚友低价的应用开发人员，但能不能和这个国家的外包商数据风险相平衡呢？”

- 检查外包商是否了解你所在的行业。你找到的合作伙伴坑农具有丰富的应用开发技巧，但是却不了解你想要开发的可以满足特殊商业或者行业需求的应用本身。

(作者：Christina Torode 译者：Tina Guo 来源：TechTarget 中国)

备份质量对风险管理策略至关重要

当把风险这个词和 IT 联系到一起时，人们首先想到的通常是：一些来自第三世界的黑客侵入了企业的网络并窃取敏感的客户信息到黑市上交易；或者是一个含有大量交易记录、信用卡号等信息的手提电脑遗失或者被盗了。这类事情一旦发生通常就是颇受关注的重大新闻。

上述这两个例子只是综合风险管理策略涵盖领域的一小部分。然而，和任何其他的商业动机一样，一个风险管理策略会反映出业务上的优先度区分，很可能一些企业会选择某些部分纳入到整体的风险管理规划中，而有意忽略或推迟其他部分。这些主要取决于特定企业更重视哪些方面。

虽然本文中不涵盖云计算相关的内容，但是其在 IT 领域内的日渐流行可能会导致当前风险管理策略的调整。如果你的企业要开发新的风险管理策略或者要对已有策略进行调整，不能忽略云计算这个新兴趋势。

备份机制决定了风险管理的质量

对任何企业来说，良好的备份机制都是整体风险管理策略中不可或缺的一部分，尽管具体方法可能各有不同。没有对关键业务信息的备份作为基础，系统恢复是不可能实现的。据统计 90%遭受关键数据丢失的公司都会在两年内受到很大影响。

考虑到备份软件的功能实现和涵盖范围的多样性——从“安装代理并备份到 Mozy”到各种完善的内部备份选项——其已成为一个不可忽视的风险管理项。

可是单单作备份是不够的。企业需要对备份质量和完备性进行日常地测试。备份工作需要严格的检测和监督，否则经常出现恶性事件。我曾经工作过的一个企业就因为 6 个月没有对财务系统进行合格地备份而解雇了整个 IT 团队。

下列几项和备份有关的事宜必须包含在风险管理策略中：

- 备份频率，对每类受保护数据的分类保存。
- 短期和长期的备份恢复目标。
- 备份流程，质量检测的频率和过程

- 备份地点 ——异地保存。

数据和网络安全

由于数据需要能从各种地点进行访问，所以数据安全具有非常重要的意义。员工可能有意或无意地在移动设备上存储了大量的数据，然后设备却丢失或被盗了。这是风险管理规划所涵盖的一个方面，必须在安全性和可用性之间进行协调。为了保护数据完整性愿意在多大程度上降低用户所拥有的灵活性？

数据安全措施由企业相关政策和所采用的技术手段共同组成。技术应该用来保证下列必须包含在风险管理策略中的政策：

- 限定敏感数据访问权限的控制机制，比如用户识别信息。
- 限定数据可以存放的设备的政策（包括行政和技术措施）。比如是否允许用户将数据存放在闪存之类的可移动存储上？
- 如果移动设备允许存放数据，则规定信息加密的政策和技术手段，比如整个磁盘和移动存储设备的加密。

另外还要注意企业的密码策略，包括密码期限和复杂度，还有用户账号的失效标准。

从可移动性的角度可以考虑诸如虚拟桌面架构（保证所有信息都存放在数据中心内部）之类的新技术，并且经常性地进行网络安全测试以评估脆弱性。

本文是本系列的上半部分中，分析了备份机制如何决定风险管理的质量，并就数据和网络安全做了探讨，在本文的下部分中将涉及物理安全和业务连续性和高可用性，并提供了风险管理的一些参考资源。

物理安全风险

物理安全是风险管理策略中不可或缺的一部分，通常包含以下方面：

- 对于诸如数据中心和中介通讯集线器等关键设备的访问控制。
- 对关键设备所在环境进行监控。比如，数据中心是否备有灭火系统以保护设备和人身安全？数据中心是否有对温度和湿度进行监测的系统？

物理安全控制对于风险管理策略的其他方面来说也是必需的，比如决定谁有权操作磁带或其他备份设备，以及谁对移动设备具有控制权。

业务连续性和高可用性

火灾、自然灾害以及其他重大事故对于企业的打击是毁灭性的。为了确保业务地正常运转，许多企业制定了复杂的业务连续性规划，以细致的步骤和举措来维持或恢复运营。由于如今技术在企业运营中承担的重要角色，确保 IT 资产的正常运转是业务连续性和可用性策略的重中之重。

高可用性是整体风险管理策略的一部分，通常包括下列举措：构建群集式的服务、对存储设备的 RAID 划分、迁移到基于 VMware 的全冗余架构。在更高一级是建设一个备份的数据中心，以便当主数据中心故障时承接服务。

如今在软件方面已经包含了大量的高可用实现，包括前面提到的群集服务和基于 VMware 的高可用方案，此外还有如微软 Exchange 2010 的高可用数据库群集（Database Availability Groups）之类的技术。

风险管理的参考资源

如果你正在筹划整体风险管理策略，可以参考下列资源来确定所需涉及的事宜、人员和方法：

- 美国国家标准暨技术学会（NIST）发布的《信息技术系统风险管理指南》（Risk Management Guide for Information Technology Systems）
- 赛门铁克公司发布的《IT 风险管理报告》（IT Risk Management Report）
- Continuity Central（http://www.continuitycentral.com/）发布的《高效 IT 风险管理》（Effective IT Risk Management）

（作者：Scott Lowe　译者：木易　来源：TechTarget 中国）

七大最佳实践打造信息技术风险管理“X战警”

不同规模的企业都面临着多方面的严重威胁，这包括来自电邮、Web、即时通信、雇员等。这些威胁的复杂性、速度和变化都在以无法预料的步伐不断发展。更糟的是，多数企业感到，它们缺乏能够正确解决这些现代威胁的资源。

多数企业会惊奇地发现，只要自己稍微有点儿警觉，或做出少许努力就会极大地减少企业遭受漏洞攻击的风险。通过问自己一些非常简单的问题，进而实施一些基本的安全过程，企业就可以快速且富有成本效益地减少其遭受风险的暴露程度。

本文阐述了现代企业风险管理的重要性以及风险管理中除简单的反病毒和防火墙之外的大量安全方案。通过洞察现代威胁，本文将帮助读者理解如何更好地保护其企业，探索业界的大量最佳方法，让企业从一个风险管理的 “挣扎者”，变成最佳的信息安全“X战警”。

威胁来自哪里

考虑到动态的威胁状况，桌面、笔记本、服务器等易于遭受Web和电邮的攻击也就不足为奇了。但威胁并不止于此。由于USB驱动器和其它的可移动存储器的存在，或可能受到意外的或故意的内部感染，企业的安全威胁总是祸不单行。普通的文档，如PDF文档，已经成为恶意软件的重要工具；简单的USB存储器感染也可能感染整个组织，并窃取数据、口令、账户信息，并将其发送给外部的攻击者。

除了这些技术挑战，更多的企业还要对付紧张的预算问题。攻击日益复杂，减少攻击的资源却又如此紧缺，企业遭受攻击的风险怎么可能不增加？对事件的及时响应又该如何做到呢？

减少风险的七大最佳实践

信息安全专业人员如何帮助企业防止这些严重的风险？可以采取哪些内部措施来防止风险？虽然不可能将风险降为零，但企业仍可实施一些最佳方法来减轻风险。这些关键的风险管理最佳方法包括：

完整的安全基础

将最新的威胁研究集成到标准的安全研究和实践中

- 拥有强化的策略

- 对自然和非自然的系统故障做好准备
- 审查日志数据
- 清理所有的感染
- 构建一个风险项目

一、完整的安全基础

期望减轻其风险的公司必须关注当前的环境，要确保自己已经部署了所有基本的安全措施。下面列示的是最基本的安全措施：

备份

企业当然要对关键部件准备好替换的硬件，而备份重要的系统和数据也是必须的。这里说两条，一是备份必须彻底充分，能够在服务器或桌面崩溃之后重建系统，或能够恢复丢失或受损的任何重要数据或系统。二是发生故障后，必须明确地分配负责恢复的资源，必须经常测试备份的可靠性。

反垃圾邮件

如果垃圾邮件不是恶意软件的主要载体，它最多会消耗带宽而不可能造成安全问题。反垃圾邮件的过滤之所以重要，主要因为它可以阻止病毒和恶意软件。任何企业，如果它运行着自己的电邮服务器，都应当确保其部署了反垃圾邮件保护，从外围设备防止垃圾进入企业网络。

反病毒

反病毒是必须的一层保护，它应当与反垃圾邮件方案协同工作。

防火墙

每个企业都应当在外围安装商业级防火墙，特别是 WEB 应用防火墙，每个桌面都应当安装软件防火墙。防火墙可以建立可疑站点的黑名单，或阻止可疑通信（如阻止那些试图向用户机器下载东西的外部站点）。

密码

好密码可以阻止未经授权的机器或账户访问。良好的口令可以更长时间地保持安全。对于共享系统，访问控制可以阻止资源被滥用。如果需要调查安全问题，日志审查可以确认任何访问。

日志

只要记录了系统访问，外发的所有数据流都被记录。应当定期检查日志，检查异常记录。

打补丁

应当定期打补丁，至少一月一次。软件漏洞一直是安全问题的一个重要根源。如今自动化打补丁已经非常成熟，这可以极大地减少工作负担。文档管理产品和媒体播放工具是现在多数攻击的主要目标。因而确保应用程序而不仅仅是操作系统打上最新的补丁是至关重要的。

扫描

应当定期扫描系统查找软件和配置漏洞，查找未经授权的软件。应当阻止一般雇员安装临时的或未经认可的软件。

二、将最新的威胁研究集成到标准的安全研究和实践中

任何企业都不能单枪匹马地战斗。为理解并应对不断变化的威胁状况，从专门研究现代安全问题的可信任的厂商那里获得一些反馈信息是非常必要的。即使大型企业也需要寻求外部源来帮助其指导安全工作。

专业的第三方安全厂商往往拥有广泛的数据中心和资深的安全专家。其解决方案往往能够提供个性化的触发器和专家分析，使企业能够合理调用资源，更好地保护信息资产。

三、拥有强化的策略

电子邮件和互联网已经成为现代企业的主要通信工具，这就迫切要求企业监视进入和离开网络的所有消息的内容。否则，可能会导致机密信息泄露，或恶意消息破坏通信，从而损害品牌和声誉，丧失机密数据并降低雇员的工作效率。

应当培训雇员，使其为了自己和企业的信息安全而保持警惕。尤其不要随便打开通过电邮传送的链接，也不要随便打开附件，或在其机器要求运行什么软件时而轻易地回答“确定”或“准许”等。要让雇员知道，恶意代码能够隐藏在任何类型的文件中，不仅仅是可执行文件中。

四、随时准备应对自然的或非自然的系统故障

电子邮件已经成为关键企业进程不可分割的一部分。为企业的关键电子邮件系统提供最多的正常运行时间是中小企业所面临的挑战之一。

传统的高可用性方法，如集群和备份等，都要求大量的 IT 专业技术，其实施成本太高。此外，拥有高可用性方案的许多公司仍会经历电子邮件的瘫痪时间。

电邮故障的真正成本，不管是计划内的，还是计划外的，也不管是广泛的或是局部的，并不仅仅反映为收入的减少和工作效率的降低。故障可以破坏与客户、合伙人、供应商的关系。故障还会导致数据丢失、遭受惩罚，或者增加安全风险，这是由于在企业的电子邮件发生故障时，用户会求助于个人的邮件账户来管理企业的电子邮件。

如果你的企业无法访问电子邮件，计划内故障与意外故障的效果是相同的。不管你的系统、员工或基础设施发生了什么问题，你的企业都应当为计划内的和计划外的故障做好准备。

五、经常检查日志数据，对最新的攻击保持警惕

不管采用了哪些防御措施，单位都应当监视其日志，查找单位外部或内部的攻击证据。日志可以提供异常的行为和失败的访问企图，这对于阻止攻击或在发生攻击后进行清理工作都很有价值。

如果不经常监视日志数据，就有可能长时间无法发现攻击者。因而，攻击者就有可能访问最敏感的数据，并使其有机会来掩盖痕迹。

六、清理遭受损害的计算机

清理受感染的机器是一个巨大的挑战。这种机器已经成为僵尸网络的一部分，或者正在将数据发送到企业外部。最彻底的方法是重新安装所有的软件，或是系统地清除将机器变成僵尸的所有恶意软件。

检测遭受损害的系统的最常见方法是，在它活动时看其发出的垃圾信息。理想情况下，ISP 会将发送垃圾信息的 IP 地址列入黑名单。黑名单技术会阻碍企业正确发送合法邮件的能力。

检测私有网络内恶意活动的一种更直接的方法是在每台电脑上阻止 25 号端口。25 号端口常被用于直接将垃圾邮件发送到互联网上，绕过企业的专用邮件服务器。通过监视由 25 号端口发送垃圾邮件的企图，当有系统从事可疑活动时，企业就可以很快发现，进而可以重做受感染的机器。

即使遭受损害的机器不会导致合法的邮件被列入黑名单，企业也需要确认并清理这种系统。因为它们还会有下面的负作用：

1、受损的机器会消耗资源，清理它们会改善 IT 的利用率，为企业省钱。

2、受损的机器会在企业的网络中产生后门，清理它们有助于单位控制对网络的访问。

3、每台受损的机器都会为全球的僵尸网络和垃圾邮件问题推波助澜，每个企业都有责任为整个社会清理受损的机器而做出最大的努力。

七、构建一个内部风险管理项目

如果没有一个正规的多功能的风险管理方案，企业会发现自己总是处于挣扎和匆忙应对阶段。强健的风险管理项目未必需要全天候工作，但它必须得到高级管理部门的支持和重视。

就不同的风险对不同的部门进行教育，提升雇员的总体安全意识是构建全面的安全理念的最有效方法。有了整个企业的支持，实施恰当的工具和进程就成为每个人的责任，从而降低了整个企业的风险。

最后，风险管理的目标应当是简化 IT 环境。正规的风险管理项目应当强化整个单位中的方案、策略、活动，确保不存在“被遗忘的角落”。将整个企业置于一个独立的安全保护伞之下能够有效地创建一个合谐的环境，这种环境要比在许多企业中的那种“大杂烩”安全方案更易于保护。

结论

威胁形势继续演变，企业的敏感数据所面临的风险也日益增大。犯罪份子在改进其攻击方法，他们有很强的耐心和智慧。网络犯罪分子更倾向于先评估目标，监视目标系统，然后寻找最佳的潜入机会。一旦进入企业的网络，攻击者就会尽可能的收集有价值的数据，并设法掩盖其痕迹。

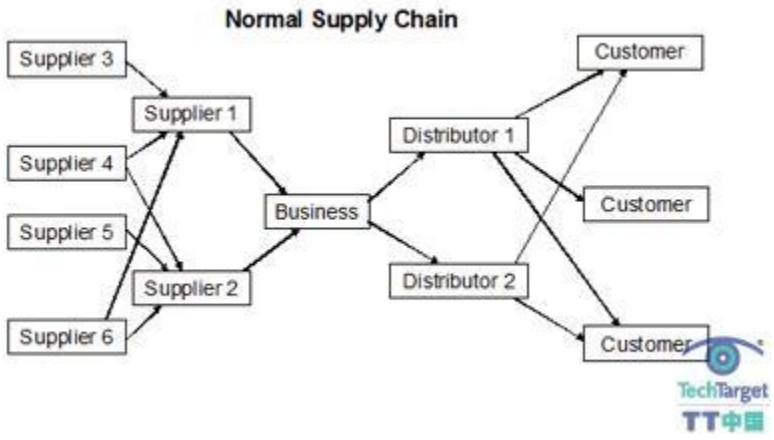
对于许多企业而言，防止攻击只是较量的一部分。另外一个重要内容是在攻击发生后，能够快速地检测它。正规的风险管理应当既能防御，又能检测。通过实施上述相对简单的进程和技术，就可以极大地减少单位的风险。当然，这些努力必须涉及到整个企业的全部人员，而不是仅仅是 IT。

（作者：茫然　来源：TechTarget 中国）

供应链风险管理最佳实践及业务连续性

通过本篇你可以了解到：几乎是所有的业务团体，无论公立或私有企业，亦无论其规模和复杂度，都有一套供应链。本篇将向你介绍业务连续性将如何保护你的供应链，以及供应链风险管理的最佳实践。

一个典型的业务供应链拓扑图或许如下图一所示。该业务直接依赖供应商 1 和 2，而这两家供应商又同样依赖于供应商 3 到 6。反过来，为了确保公司产品按时送达客户，公司的业务也依赖于分销商 1 和分销商 2。这是一个最通常的模式，我们可以在这条供应链上清晰地看到许多相互依赖的痕迹。



图一：一套通常的供应链

如果你正在考虑如何管理供应链的风险，你或许可以引入业务持续性管理技术作为风险识别、降低风险以及恢复流程中的一部分。

供应链的风险管理调查

2009 年秋，业务持续性机构公布了一项调研报告：

- 在 201 家企业反馈中，3/4 的受访企业在过去 12 个月中遇到过供应链中断。造成中断的最主要原因有经济衰退，H1N1 全国性流感，以及来自 IT/电信的业务中断。

- 业务中断主要会影响生产，而损失营业额，客户投诉和产品上市推迟的问题也同样普遍。

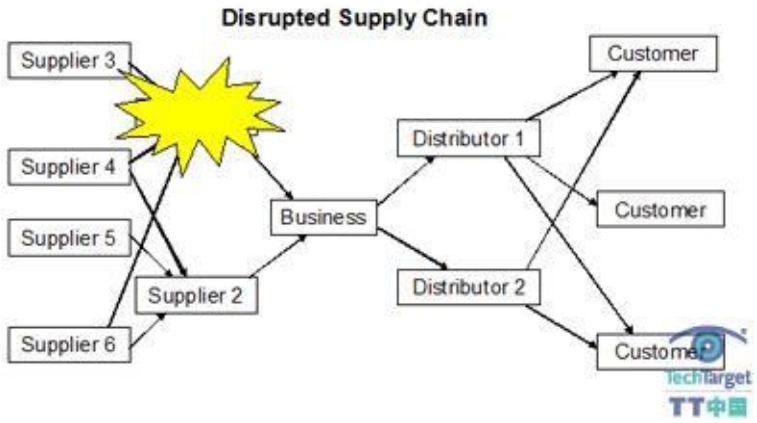
根据 Aon 2009 年 21 世纪供应链风险调查所示，接近 3/4（74%）的业务正在着手采用供应链风险管理。这项调研的主要结论有

- 超过半数的公司与其供应商发起了定期沟通机制和审计策略。
- 调查供应商的供货商来增强供应链的受访公司的数量增加了 20%。
- 即便保险仍是风险管理策略的首要因素，只有少于 20%的企业使用保险作为其转移风险的策略。
- 十分之一的公司强调对于道德问题的评估（诸如培养一种符合规范的业务）以及按照其表现给其供应商的相应行为准则行事。
- 55%的受访公司承诺目前没有关键的性能指标来监控供应链风险管理情况。

在供应链中引入业务连续性

正如每家公司都会面临威胁和风险，都有各种不安全的因素；对于供应商伙伴而言，事情同样如此。每家供应商都会遇到这类风险情况，比如火灾、洪水、技术故障、电力中断或其它的因素。

而通讯故障、运输系统中断、互联网暂停服务、以及由疾病或罢工而引起的工时损失等都会影响每家公司及其上游和下游供应商，还包括最终客户。当你开始添加所有这些，你会突然发现为什么供应链是业务连续性管理的主要因素。



图二：一个中断了的供应链

上图中描绘了当供应商 1 无法提供货物或服务时的业务情况。暂且不论其产生原因，业务必须从现有供应链中调整以弥补供应商 1 处得损失。不过供应商 2 是否承担得住呢？假设供应商 2 无法接手供应商 1 的这部分业务，供应商 3 到 6 是否可以帮得上？这些问题必须有一个答案。而有效获取足够信息的方式之一就是业务冲击分析（business impact analysis 简称 BIA）。

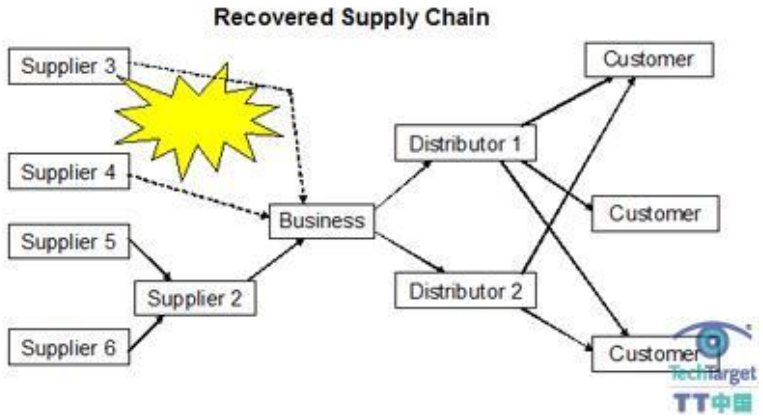
BIA 中的核心工作有 1）识别出内部和外部有相互依赖性的公司，并且 2）记录下这些依赖性中如果有任何中断，其对财务和运营的影响。这类工作可以是一个内部和外部的结合，对于供应链是一个理想选择。

从供应链中的外部成员的角度看，首先你必须识别并描绘出整个供应链关系图。其次，借助你公司核心成员提供的信息，对各供应链中成员分配各自重要性的权重（例如，核心应用占 5，非核心应用占 1）以及财务影响（例如，每个月公司支付给某特定供应链成员的费用）。以此分析你公司是否正依赖一些没有列入统计的供应商，比如一个核心供应商依赖某家物流公司，并且分析这家物流公司对你的公司有多重要？

以上这些工作都可以使你建立起你自己的供应链风险地图。结果最为笼统的图就可能会像上图一那样，不过图一里也有较详细的供应链和联系描述。这些分析可以帮助你识别供应商中潜在的风险点，这些供应商依赖的上游供应商以及供应链之间各供应商的联系。

供应链风险管理策略

当你建立起供应链风险管理的最佳实践时，对任何业务连续性和/或者是风险活动，你都必须用文档记录下来，将其教会处理故障情形的员工，带领他们经常演习（最好也能叫上供应商一起）并定期回顾复习。



图三：一个回复供应链的示意图

图三描绘了一个中断了的供应链如何重新配置，并在一定程度上回复了原有的功能。由于供应商 1 退出了供应链条，供应商 3 和 4 现在将直接为公司业务提供产品和服务。为确保这种回复工作顺利完成，必须进行仔细地分析有风险的业务供应链，并识别出可以维持住供应链的任何机会。

除了业务连续性，另两项选项也应当在涉及供应链风险和供应链迁移时加以考虑。

1） **风险管理**——通过绘制整条供应链地图（图 1~3）及其依赖性，开始进行供应链风险管理工作。同时，诊断威胁、风险和供应链的软肋；并识别出单点（甚至多点）故障点。其次，部署策略来消除或降低这些问题。需要记住的是，这是一项持续的过程，并可能需要采用特定的产品化的软件，比如 Epicor Manufacturing、Infor ERP、Microsoft Dynamics ERP 以及 Oracle E- Business Suite。

2）**保险**——种常有但是错误的想法是供应链风险可以通过业务中断险得以缓解降低。不过，为避免业务中断险的保额问题，一些公司仍从包括 Aon 和 Zurich 保险商处购买特定的供应链保险单。

供应链风险管理和业务连续性是一对合作伙伴。业务连续性话题在全球范围快速成为热点。

供应链执行过程中最大的挑战在于是否能够快速识别出公司业务运作中每天的影响因素，并对其进行评估管理。快速地识别危机前的情形，评估可能出现的业务中断场景及其影响，然后积极响应，防止或减缓业务中断对供应链的影响，这些都是公司的供应链处理灾难情形，最小化业务中断影响的能力。

请参考：

探讨业务连续性标准和实现技术

（作者：Paul Kirvan　译者：张瀚文　来源：TechTarget 中国）