企业风险安全管理

企业风险安全管理

企业风险安全管理的需求正在推动身份识别管理和内容监视等技术的发展。但是，有太多的企业正在依靠技术而不是政策来处理风险管理问题。风险管理是种关键推动因素，你需要搞清楚需要做什么，而且应该把钱花在什么地方……

云计算带来的企业风险

“云”过去常被用于对各类基于 Web 应用的通称。现在它普遍用于指网格或实用新型计算模式，在这点上它取代了本地硬件和存储器输入/输出。企业正在纷纷向云这个方向发展，只是一些企业比另一些发展的要快。然而，转向云这个方向使企业面临许多需要去考虑的风险。这些风险的核心在于许多云/ Web 2.0 的供应商无力满足法律与规章的要求。

- 请准备好迎接云计算风险管理的挑战
- 云计算需要考虑的三个风险

企业风险管理最佳实践

IT 工作领域中有许多的最佳实践，企业风险管理也不例外。我们在控制企业的风险工作中总结出了以下一些最佳实践：

- 基于风险的多重身份认证的最佳方案
- 进行 Rootkit 风险评估的最好方法是什么？
- 如何撰写结合业务、安全需要的风险方法论（一）
- 如何撰写结合业务、安全需要的风险方法论（二）

企业风险管理的文档操作

在管理供应商合同的时候，非常重要的一个环节是将过程化考虑进去。订立合同不是孤立地去承诺某种义务，而是企业风险管理中综合信息安全计划的重要组成部分。将风险管理策略文档化有助于提醒金融机构“应该”考虑某些类型的合同保护。

- 供应商合同管理：基于风险的监管指导
- 供应商风险管理：过程化和文档化

风险评估和管理策略

想想你们公司有的基础设施有多大可能正被不怀好意的黑客盯上。你的基础设施的信息具有多大的价值？该怎样阻止黑客窃取你的信息呢？你可以开展一个员工意识和公司风险评估策略的培训，风险评估是信息安全的核心。为了保护系统，必须决定风险的等级。风险等级越高，就越需要保护。风险评估包括对 IT 架构的三个部分的评估：威胁、漏洞和风险。

- 如何防御黑客窃取信息：员工意识和风险评估策略
- 外包安全服务的风险
- 风险评估应该包括哪些步骤？
- 社交媒体：金融机构的风险管理策略

请准备好迎接云计算风险管理的挑战

随着信息安全项目经理开始新一年的工作，他们通常会找出那些能够影响企业安全策略的关键主题。

然而，毫无疑问有一个主题比其他主题都突出：云计算。艰难的经济环境确实令云计算很有说服力。因为按需（on-demand）资源是动态可扩展的以及动态灵活的；按需资源已经是2009年的热点了，它总是吸引着大型或者小型的企业。不管2010年的经济状态如何，云计算肯定会继续改变着我们的IT方式。

对于那些想要保护企业的网络用户和数据的人来说，往云计算转变将会是一个很大的改变和挑战。规则遵从最有可能阻止企业把所有的数据和操作都转向云，所以除了保护现有的网络基础设施以外，这个转变实际上是另一个在安全领域上的挑战。转向云计算意味着需要把数据以及应用程序都放在外围防御保护和物理访问控制之外，越来越多的用户将不受HR的控制，比如供应商、客户端以及合作伙伴等，人们将通过基于网络的协作工具来访问你的数据。IT管理员对于保护那些能够访问公司网络的移动用户的安全已经很头疼了，但是这一点对于云计算而言是一种完全不同的规模。

对我来说，关键的安全挑战之一是：怎样才能有效的管理和执行处于企业防火墙以外的员工、顾客以及合作伙伴的访问控制。云计算让我们都成了远程工作人员，而根据定义，云的应用程序和数据也处于企业的外部。这就意味着你不能再依靠那些多重认证技术、防火墙以及其他的外围防护措施了。

从战略上讲，管理这些挑战需要采取若干行动。HR的安全政策必须重新复查并且加强，以确保这些这些政策可以执行强有力的用户周期管理。你还必须有一个详细的身份识别以及访问管理策略，这个策略要能够充分利用联合的身份识别管理，它是一个能让用户通过自己的安全域安全地访问数据或者系统。我建议在你自己的企业应用程序中能够使用单点登录（SSO），并利用这个结构来简化云提供商的集成和实施。

云计算将更多的依赖于互联网连接，因此，就算是比较小的操作也需要建立某种形式的冗余以确保数据和应用程序在任何时候都可用。尽管进行了大肆宣传，但是云服务还是相当的不成熟，很多人都经历过某种形式的中断或者其他的毛病。有些云很容易失败，它只是糟糕的经

济环境中出现的一个新行业。多重服务提供商将向你通过更好的网络多样性以及业务连续性，所以任何基于云的工程都应该包含供应商中立的应用程序和数据结构。这包括以独立的云形式进行备份，以及一个独立的机器镜像（machine image）。你需要尽可能直截了当的进行这一转变，或者执行必要的应急计划，准备随时把所有的操作都拿回到内部云中进行处理。尽管云计算会减少一定的连续性问题，但是它永远不可能避免对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将会受到更多、持续时间更长的攻击，因为它们是黑客和网络恐怖分子喜欢的目标。因此，建立一个数据加密策略并且实现某种技术对它进行支持是最好的主动防御措施。从本质上讲，加密了的数据是受到保护的，这也是为什么许多法律法规都要求这样做的原因。所有的数据和网络通信都应该加密，即便是其他的服务会对它们进行保护。加密还可以让你将角色（roles）和数据分开，因为加密密钥可以控制着对数据进行访问的权限。

在新的一年，我们一定会看到许多新的基于云的服务上线，很多服务会给企业带来实质性的经济利益。有些服务无疑将会改变过去长期建立的风险回报关系，所以当你评估转向基于云服务的投资回报率（ROI）时，你需要重新检查企业的风险业务策略和承受能力。云计算正在改变 IT，所以在 2010 年，请认真考虑如何把安全嵌入到新的业务程序中去，以便基础设施、数据和用户都能得到保护。

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

云计算需要考虑的三个风险

“云”过去常被用于对各类基于 Web 应用的通称。现在它普遍用于指网格或实用新型计算模式，在这点上它取代了本地硬件和存储器输入/输出。企业正在纷纷向云这个方向发展，只是一些企业比另一些发展的要快。然而，转向云这个方向使企业面临许多需要去考虑的风险。这些风险的核心，是许多云/ Web 2.0 的供应商无力满足法律与规章的要求。以下是三大主要风险：

1．安全：对于许多企业来说，信息的安全性是最主要的风险。这或许是受到了保护知识产权、商业秘密、个人可识别信息或其他敏感信息这些需要的驱动。要使这些敏感信息在互联网上可用，就需要在安全控制以及内容访问和信息途径的监测上有重大的投资。一些供应商提供的日志记录和审计控制还不能像企业内部及企业应用程序所提供的日志记录一样健全。在这个方向上的困难是，要确保在事故发生后，企业能够知道是谁访问了文件以及可能对文件所做的操作是什么（如编辑，下载，更改访问等）。

2．电子化搜寻（E-discovery）：电子化搜寻当前的趋势大多是假设企业已经明确知道它的信息存储在哪里，这些信息如何备份，以及如何保护。这些规则也假设企业能够实际地检查存储设备，并且在必要时，能够检查存储介质来获取擦除及/或删除文件的证据。在云环境中，企业可能很少或者根本不知道存储和备份的过程，也很少或根本不会亲自去访问存储设备。而且，由于来自多个客户的数据可能存储在单个存储库中，对存储介质的取证检查以及对文件存取和删除的正确认识将是一个重大的挑战。

3．计算机取证（Computer forensics）：对许多企业来说，计算机取证是电子化搜寻和内部调查的关键组成部分，而且经常需要实际地访问存储设备或计算资源。从计算机操作系统存储在物理和易失性存储器里的信息中，我们可以了解到很多东西：存储在计算机的随机存取存储器中的信息在关闭计算机后几乎会立即消失。当数据和应用程序脱离本地个人计算机时，取证调查人员可能就不能再访问某个案例的关键信息。一个特定的文件或此文件最后被访问时的地点，通常在决定该文件如何被使用以及被谁访问时起着关键性的作用。假设数据存储转移到云，而数据又没有完全消除的话，那么获得未受污染的证据数据副本的能力可能会降低。

预先准备

虽然这些问题可能不会是云环境中移动数据存储和应用的绝对障碍，但它们已明显妨碍了工作的正常运行，这导致企业需要认真审查其合同义务、风险预测、安全基础设施和监督能力。企业应该准备好向供应商提出适用于自己商业需要以及存储和交易信息种类方面详细的安全和法律要求。

今天的一个主要挑战是，几乎不存在涉及到在云环境中存储信息的法案（case law）。企业必须采取措施来依法保护知识产权和信息的安全。由于这一领域缺乏相关的判例法，法律部门也可能会担心云环境中知识产权，商业秘密和合法的特权信息（privileges information）。在任何情况下，企业必须保证将其安全和法律规定作为合同的一部分，并进行定期审计，从而确保供应商能够满足这些要求。

（作者：Patrick Cunningham 译者：Sean 来源：TechTarget中国）

基于风险的多重身份认证的最佳方案

身份验证和访问管理（IAM）——这种用来管理用户信息和用户、网络以及应用程序之间关系的技术——最近引起了更多的关注，强大的多重身份认证手段已经成为企业 IAM 战略的核心部分之一。

多重身份认证经常是开启 IAM 旅程的第一个端口。众所周知，仅仅依赖密码进行保密存在很大的风险，所以定期更换密码是大家很容易想到的解决方案。而多重身份认证则排在企业现已采用的 IAM 组件列表的首位。

尽管公司高管们对这种多重身份认证手段的概念感到满意，但是对于安全和风险专家来说，让高管们提供必要的资源支持才是真正的困难所在。Forrester 研究公司最近调查了很多已采用了多重身份认证的公司，以了解这种方案的最佳执行方式。在这次调查中，出现了以下四个优秀的方案：

1．了解用户是如何工作的

最佳安全方案是用户实际已经采纳的方案——让用户接受安全方案的关键是使这些方案尽可能不对用户的正常工作造成影响。安全方案不应该仅仅是 IT 系统上的一个事后才体会到其重要性的部件；相反，强大的安全认证措施必须尽可能地融入到员工的日常生活中去。

各大公司应该正确评估安全认证方案对其用户产生的实际效果。深入了解用户如何工作并对特定用户每天的工作进行准确的描述，是确保员工工作效率的关键所在。良好的沟通是用户最终是否适应的关键——包括提醒他们实现采取正确的改进措施——而这与所选择的技术无关。

和其他大规模的技术项目一样，不完整的研究、不充分的测试以及薄弱的授权会把多重身份验证的实现变为昂贵的负担。通常，这些都是技术方面的问题，但发生在人事方面的问题也同样麻烦。例如，安全机构有时会将 IT 员工与特定用户混淆。虽然以安全的名义在 IT 部门及高层用户组织中进行一次试点工作是比较容易的，但它会导致时间和金钱等方面的资源严重估计不足。

2．确定合作方的需求并预先采取行动

在商业活动中，多重认证可以看成是一种没有 ROI 的不可复原成本——这是一个当安全项目朝着与 IT 无关的方面倾斜时全球 CISO 们都会面临的问题。安全专家需要查看客户公司的每一个角落，从而提出可以表明客户需求的 MFA，并了解客户正在试图解决的业务问题。很明显，这不仅涉及到应该运用何种技术的问题，而且涉及到多重身份认证项目如何在内部开展。由于行业的纵向差异，确保遵从法规可能是一个更强大的营销方式，但这样会让项目面临一直延期到最后截止日期的风险。因此，试着将用户数据与项目结合并加以保护是一种非常有竞争力的方案。

许多 IT 人员对待任何事物都有这样一种倾向：看它是不是可以解决安全方面问题的技术手段——这样做可以在处理人和程序之间的关系时，解决不确定性问题。然而，让 CEO 们对这种方法有一个清楚的认识，或者叫他们尝试着去理解 MFA 解决方案的精妙之处，常常会让他们的目光变得呆滞。当你试图将一个 MFA 的解决方案出售给高级主管时，不要把它当做一个技术方案；恰恰相反，你更应该把它当做可以保护公司数据的商业方案。

3．提前预判，减轻技术上会遇到的挑战

在 Forrester 所调查过的所有人中，即使他是拥有丰富经验的 IT 安全专业人员，在处理多重身份认证的问题时几乎都会遇到一些意想不到的技术问题。他们对此的建议是什么呢？有如下几条建议：使用现有的技术解决它们；对现有系统进行详细的分析；不要低估项目所需的时间和资源；越早进行测试越好。测试是顺利解决问题的关键，并且次数越多越好——这样做的原因更多是为了避免匆忙就启动项目。不仅如此，测试将揭露意想不到的系统问题，包括需要更换过时的技术，如传统的物理访问系统或远程访问软件。

很轻松的就让现有部署了的技术通过评估，或者是认为一旦 MFA 投入使用，现有的技术仍然可以继续使用，那么这将对系统的使用造成不良的影响，例如项目的推迟不可预知，以及没能预计到与将来的技术不可兼容。不要成为忽视测试的牺牲品！

4．制定策略，在正确的时机得到支持

尽早开始内部的销售过程，并且尽快得到高层的支持。后者通常说起来容易做起来难，但幸运的是，近年来安全问题终于获得了应有的 C 级重视。密码作为连接 IT 资源的唯一手段，它的使用存在着巨大又显而易见的安全弱点——应该把它在历时多年、拥有多个项目的 IAM 计划中置于优先地位。公司一旦引进，不要因为无法交付、或在回扣上做出过多的承诺而损害了自身信誉。

在这里，可用性是一个值得重点关注的问题，而它在赢取用户的支持上也显得非常重要，否则在项目交付后，你很有可能会耗费大量时间与那些对技术不感兴趣的客户进行交涉。对于大规模的首次展示，在起步阶段你应该着手获取来自公司上下所有重要员工（团队负责人、总监、顾问等）的支持。当然，其中肯定会存在批评和抵触情绪——因此首先应进行大量的研究，为核心用户选择合适的技术，并征求他们的改进建议。

这在将来会显示其自身价值的。

（作者：Bill Nagel 译者：Sean 来源：TechTarget中国）

进行 Rootkit 风险评估的最好方法是什么？

问：进项风险评估的最佳方式是什么？特别是针对 Rootkit？

答：Rootkit 是很多想要访问受害者系统的攻击者选择的工具。有了这种恶意软件，攻击者可以在受害者的计算机上安装恶意代码，而用户很难检测到这种方式。

目前，有很多种 Rootkit，可以在任何操作系统上使用。研究人员已经发现了一些有商业用途的 Rootkit，他们是为用户设计的，为了以极小的代价逃避很多杀毒厂商。

当处理 Rootkit 和恶意代码的时候，很多安全专家都关注工具和技术。虽然这一点很重要，但是它还没有和开发安全团队的处理 Rootkit 能力更重要。

当我为了证书和鉴定合格而努力的时候，我希望设置一种情况，在这种情况下我可以在一个系统上安装 Rootkit 并要求安全团队识别并移除它。我系统查看安全团队处理现场的情况，而不是依赖存储的程序或者定期更新杀毒程序的证明。

至于技术，我喜欢 F-Secure Corp。的 BackLight 工具 RootkitRevealer，以及免费的 IceSword。在处理 Rootkit 的时候，存在第二个（或者可能甚至市第三个）选择非常明智，因为 rootkit 在不断进化，可以绕过 Rootkit 检测技术。

（作者：John Strand 译者：Tina Guo 来源：TechTarget中国）

如何撰写结合业务、安全需要的风险方法论（一）

保护信息资产是信息安全计划的头等要务。但现在没有做到这一点，这要怪业内那些不恰当的策略；而整个行业似乎却满足于目前的策略。我们让供应商和一些条条框框指导我们该如何保护信息资产，而不考虑去分析一下实施我们打算要采用的技术可以把什么风险降到最低。如果我们完全信任了对信息资产保密性、完整性和可用性（CIA）的保护，那么就必须跳出框框花时间来分析风险，并设计可降低其余的风险的安全系统。

尽管在周边的安全防护和遵从上投入了大量的资金，但还是有安全漏洞涌现（例如 ChoicePoint 公司累计总共丢失了超过 2 亿 6000 万条记录;光 2008 年就丢失了 3000 多万条）。目前用于保护我们信息资产的标准和条例与我们的技术并不相符，也没有充分缓解当前面临的威胁和安全风险。很显然，再多花钱在技术上于事无补，花钱制定治标不治本的条例或计划也同样不起作用。

风险处理必须抓住安全这个根本原则，并集成到一个安全计划中，安全计划要综合考虑到业务需要、必要的关注点、当前攻击媒介，还要满足法规和合同的要求。遵从标准和规定有助于确定哪些应该关注，但它不应成为安全计划的推动因素。想解决所有的威胁和弱点是不可能的。减少其余的风险，而非那些陈规陋俗，才应该成为指引开发、评估工作，以及在机构内提高安全实践的驱动因素。

各个组织必须遵循风险方法论;我们将在这里介绍一套，这套方法论是作 Nova Southeastern 大学博士风险管理课程的一部分发展起来的。James F. Broder, George L. Head ,Stephen Horn, Elaine M. Hall, 还有 Thomas Peltier 的研究成果也作为方法论发展的一部分进行了探讨。

在过去的两年中，这一风险方法论进行了修订，并且在一个私人公司和美国华盛顿大学（University of Washington ）得到了实施 。它现在完全融合到了华盛顿大学的信息安全计划中了。由于成功把业务价值、策略以及运作整合到了华盛顿大学的企业风险管理(ERM)计划里，这一风险方法论最近在华盛顿大学关于企业风险管理 (Enterprise Risk Management ,PACERM)的董事咨询委员会(President's Advisory Committee)上被提了出来。

这一方法论是基于我们四年前开发的一套安全框架。这套框架囊括信息安全的方方面面，处理所需的各种安全标准和规定，并且把信息安全整合到了业务策略当中。这个框架的最初设想的提出经历了许多前期工作，包括与几位安全专家探讨，重新检查 PCI-DSS, HIPAA, Gramm-Leach Bliley 这些现有的法规和 ISO 与 NIST 出台的标准；还审计了十多个公共的、个人的、政府的信息安全计划和实践；并且还把对安全框架的调查作为了理科硕士信息安全计划的一部分。

这个项目的目的就是开始出一套可以与信息安全计划相集成的框架，这个信息安全计划要能帮助维护本组织的信息安全行动，表现出达到或者超出“适当关注”原则，并且满足本组织的战略安全的需要。

该框架按照战略、战术和运作划分为 13 个元素。该框架对安全计划来说是不可或缺的，因为需要它来对整个组织进行全盘的清查以找出危险的部分。该框架使得组织有能力修改或增加控制项，并使得风险降低到可接受的范围。它还为组织内的信息安全实践发展、评估和改进提供方向。整个安全计划范围内都必须处处贯彻安全防护的意识，以灵活地应对新的威胁。遵从标准和规程是很重要，但单单是遵守这些规程并不意味着其余的威胁就会减少。

综合的风险方法论

风险方法论要求每年重复进行自主的质量评估。例如，华盛顿大学就每季度都要完成一次风险评估并把结果报告给安全指导委员会。

如果没有一种切实易用的方法，人们往往会推脱或者不去做评估，采取一种被动姿态，或者错误地执行这个过程。风险评估只是对一个时间点的评估，很容易失去时效性。为了有效地减少风险，安全专业人员必须定期评估其组织的安全和风险状态。

Jan Emblemsvag 和 Lars Endre Kjolstad 在《Qualitative Risk Analysis: Some Problems and Remedie》中论述了安全风险评估如何取决于对组织的能力和信息质量的一贯分析，而且分析是在有丰富的知识和有资质的专业人员的前提下进行的。如果没有一个一贯的方法，没有对组织的能力的考量，没有对评估信息的质量进行认真分析，那么质量评定的结果还得打上一个问号。据 《Advances in Statistical Methods for the Health Sciences》的作者 Ruth Hauser, Eric Breidenbach 和 Katharina Stark 说，即使质量评定有局限，他们依旧可以为风险决策提供足够的、其它方法所无法取得的信息。

评估方法是基于一个前提，即风险的数量是取决于组织保护信息资产免受威胁的能力有多强。下面这个公式可以体现出这点：随着组织保护信息资产的能力提升，或者组织所面临的威胁减少，整体的风险分数就要降低。计算风险分数需要组织基于全面的安全要素框架评估他们的能力和威胁。必须为每个安全因素都确定关键指标和威胁，这样才能对能力和威胁的可能性、影响进行评估。

这一风险方法论可以把信息安全计划集成到组织的企业风险管理（enterprise risk management ERM）计划中。这是通过确定风险陈述和指标以及各个安全因素内的威胁来确定的。风险声明被归为四个方面，包括：

- 合规（未能遵循法律，法规，合同协议，标准，或组织的策略）；
- 财务（亏损的实物资产或财政资源）；
- 运作（影响正在进行的管理程序）；
- 战略（影响到能否实现目的或目标） 。

指标、威胁和风险声明之间的关系使得组织能够从风险因素的角度和企业风险管理的角度同时对风险进行评估和检查。这确保了定性风险评估所需的一贯的自顶向下或自底。这个图表显示了企业风险管理和这个框架之间的关系和框架。

(作者：Cris Ewell 译者：Sean 来源：TechTarget中国)

如何撰写结合业务、安全需要的风险方法论（二）

如何鉴别风险

对安全风险、目标和威胁的鉴别对于安全风险的处理是至关重要的，也是组织应该做到的第一步。风险鉴别阶段不可掉以轻心，且需要由有资历，有知识的安全专业团队作出团结一致的努力。这个团队必须熟悉业务环境，安全标准，业务需求，规程要求和当前的威胁范围。在这个阶段，该团队将确定并验证主要指标以及当前环境下的威胁。讨论每个指标和威胁非常重要，这可以确保它们既代表了每个安全因素，又不至于啰嗦。

风险陈述可以在该组织的企业风险管理程序中创建，或者如果没有一个协同的风险程序的话， 就单独创建。该团队必须从根本原因上考虑，而不能只着眼于风险的影响或是降低风险的措施。在团队完成指标、威胁和风险陈述的定义工作后，每一个指标和威胁都将与风险陈述中的一个或多个关联起来。安全陈述、指标和威胁之间的这种联系，使得组织可以分析能力和威胁的变动对风险造成的影响。在这个阶段几次返工也是很常见的。团队为每个安全因素完成了指标和威胁的确定之后，这威胁与保密性，完整性和可用性（CIA）三元组之间的关系也应该就确定了下来。进行风险鉴别这个步骤的目标是为了在各个安全因素之间得到比较平衡的指标和威胁，并明确与安全陈述之间的关系。

如何评估风险

在风险评估阶段，该团队将使用主要指标和威胁作为评分依据。千万谨记，生成结果的那种方法的一致性和团队的专业程度比分数的定义要更为重要。团队必须记录其决策过程，以确保一致性。保持一致性的好处是能够比较过去和现在的评估并分析其趋势。

这个阶段的第一步是确定组织在为每个安全因素制定详尽的安全计划这个过程中达到了何种水平的能力。有一个 5 级能力标准可以运用于这个过程。

该团队也将评估每一个安全威胁因素的可能性和影响范围。威胁客户也应和数据资产一起考虑到这部分的得分中。威胁客户是那些可以利用各种威胁资源利用安全弱点的人。实施攻击的企图、能力以及机遇会使得一个人成为威胁客户。潜在的威胁客户可能包括雇员，承包商，前承包商和分包商，维修人员，前雇员，以及未经授权的外部用户。

可能性和影响按三等打分（低，中或高）。对可能性的得分造成影响的有威胁客户的能力、当前采取的控制措施，还有攻击的类型和频率。造成的影响取决于利用安全弱点对资产和组织所造成的损害。衡量损害的方式有崩溃、损失竞争优势，能力和信誉的损失还有资产的重置成本。

最后的威胁指数评分计算方法是把可能性分数和影响分数加起来，再为该威胁与保密性，完整性和可用性（CIA）里的每点联系加上一分，最后得到总的威胁指数。如果威胁仅仅是和可用性相关，那这一分就会加到可能性和影响分数里去。如果与 CIA 三元组里的每一点都有关系，那么就会加上 3 分。基本安全指数得分最高是 9 分，最低是 3 分。威胁评分的计算是了为了解每个安全因素的威胁。能力评分的计算是为了了解每个安全因素里的指标。威胁得分的威胁因子初值是设为 1.0，除非该组织认为某种特定的威胁权重要更高一点，才可以给这个威胁因子额外加上 0.1 到 0.5。

如何分析和减轻风险

这个阶段评估风险识别和评价阶段收集到的信息。分析从查看当前和之前的整体安全处理能力得分和威胁指数得分开始。随着时间的推移，就可以建立起有助于分析的发展趋势图。这一趋势将有助于该组织确定需要完成哪些步骤以提高整体安全状况，减少威胁的影响和可能性，降低该组织面临的风险。应当特别注意威胁指数分数高，能力分数却低的安全因素。这种反差造成更大的业务风险，应当设法降低。

最后一步是建立一个风险缓解计划并确保该计划与安全战略计划挂钩。该战略计划和项目所依据的是风险和有针对性的安全指标。减少风险的项目与遵从标准的努力之间的冲突可能会在分析过程中被发现。管理层需要统一这些差异，确定行动方针。分配资源时，最应优先考虑那些有高危漏洞的东西。这些方面需要立即减少风险，以保护企业的利益和任务。我们的目标是尽量减少组织面临的总体风险。

减轻风险的计划应包括使能力与风险相当，推荐的控制措施得到实施，确定控制措施的优先次序制，落实所需资源，开始和预计结束日期，以及正在进行的维修和操作要求。理论上说来，应该每个季度进行风险评估以跟踪降低风险计划的进度。风险陈述应该体现客观能力和威胁的趋势。元素那一栏下的颜色表示当前特定元素的风险级别。目标栏下的的颜色（红色，黄色或绿色）表示当前预算周期内，现有能力和目标能力之前的差距。红色箭头表示的消极变化（威胁的增加或能力的降低），白色箭头对应于一个积极的变化。另外还应与安全团队进行讨论，以评估风险是否可能通过目前的项目降低，或者说是否需要作出改变。

风险沟通与监测

有知识，有资质的安全专业人员需要定期讨论信息安全风险问题。在有限的资源和预算的情况下，重要的是要确定风险和能降低风险的补充控制措施。应该要做出一份季度风险报告样本来体现这些风险上的变化，并向高管们传达这些变化。。能力级别有三条线。里面那条线（蓝色）表示目前的能力，中间那条线（红色）表示当前预算年内预计的增长能力，还有外面那条线（黑）表示每个安全元素所期望达到的长期能力目标。威胁指数评分显示当前每一个安全因素的威胁。这些图表是在团队输入能力和威胁分数后计算出来的。每个风险陈述（用 O1, C1, F1, S1 等来标识）和各个安全因素在他们的个人风险评分的基础上被标在了这张风险图上。安全因素线使用的关键指标与能力水平一样。从过去一段时间以来在能力水平、威胁指数分数和风险分数上的变化都在中间的方块中表示了出来。这份风险管理报告很好地概括了当前的风险，趋势和安全计划里的不足，并应当用在有关战略和风险缓解计划的讨论中。

风险管理要全面

安全行业需要跳出樊笼思考， 采取能降低风险的安全策略，并且还要能直接分辨出哪些降低风险的方法能有效打击对手。仅仅依靠技术或是依靠外围防护，自我假设敌人会被阻挡在外，都是无法解决企业的信息安全问题的。要解决这个问题需要采取全面的安全计划，把风险管理作为整个策略的驱动力。现状已让人不堪忍受，我们整个行业必须改变做法， 并运用新的思想， 如违约假定、积极响应、攻击能力和情报分析，此外还要对我们的对手在风险管理策略中的采用的攻击的攻击媒介和方式进行有针对性的讨论。

(作者：Cris Ewell 译者：Sean 来源：TechTarget中国)

供应商合同管理：基于风险的监管指导

尽管很多监管指导的出处都是针对金融机构的信息安全合同要求的，这些要求的主要特点是他们是灵活的，基于风险的。也就是说，这些指导原则避免了指定在每个合同或者合同要求（例如某种加密标准）中使用某些技术。通常，这些指导原则甚至都不会使用“必须”这种词语，而是提醒金融机构他们“应该”考虑某些类型的合同保护（当然，那些和银行监管者打过交道的人知道他们所说的“应该”有的时候并不意味着那是可选择的）。

重点是，尽管需要某种形式的书面合同来保证供应商对用户信息的安全负责，监管组织担心的主要是预先通知的风险评估，例如，确保金融机构将风险级别作为对供应商的系统化考察流程的一部分，而且合同中需要合理并妥善的安全性度量，这里的合理基于已知的风险因素，例如和供应商共享的信息数量和性质。典型的基于风险的架构例如《Interagency Guidelines Establishing Standards for Safeguarding Customer Information》（《客户信息保护标准建立联合准则》），它于 2001 年由联邦银行机构和联邦贸易委员会联合起草，用于实施 Gramm-Leach-Bliley 法案（金融服务现代化法案）的安全要求。就合同而言，这一准则要求金融机构要“以合同形式要求它的服务提供商采取合适的方式保证符合这些指南要求的目标……”（例如，执行保护手段来降低发现的风险）。

其它的联邦准则增加了一些特定的信息安全要求，但是这些都是最基本的。例如，针对国有银行的第三方风险管理的 OCC 公告第 2001-47 号，就提供了银行需要考虑的合同条款的详细总结。在信息安全这个问题上，公告除了通常的保密措辞和对实施合适的安全措施的要求之外，还指出银行应该要求供应商向其透漏造成未经授权入侵的，并可能会实质性地影响银行和它的客户的安全漏洞，还有要报告这种入侵的影响和采取的补救措施。2004 年美国联邦金融机构监理委员会（Federal Financial Institutions Examination Council - FFIEC）发布的《Outsourcing Technology Services IT Examination Handbook》（外包技术服务 IT 审查手册）也重复了这一要求。

2008 年 6 月发布的《FDIC's Guidance for Managing Third-Party Risk》（FDIC 的第三方风险管理指南），也有类似的条款：“处理机构客户的任何非公开的个人信息都必须符合机构自己的隐私政策，而且要符合适用的隐私法律法规。任何对安全性和保密信息的入侵，包括非授权入侵引起的潜在泄露，都应该被要求迅速并完全地向金融机构公开。”

在监管机构发布的准则之外，金融机构可能还要遵从国家数据安全法律和《Payment Card Industry Data Security Standard (PCI DSS 支付卡行业数据安全标准)》。这些地方指出的合同要求也是最低限度的。例如，2009 年 8 月对马萨诸塞州规定 201 CMR §17.00 的修改使其符合了上述的跨部准则；拥有或者被授权使用马萨诸塞州居民个人信息的机构必须以合同形式要求第三方供应商实施并维护符合法规和联邦法规的合适的保护性安全手段。（不过，任何在 2010 年 3 月 1 日前签订的合同即使缺少这些条款也不会被认为是不合标准。）

PCI DSS 第 12.8 号条款指出如果持卡人的数据被共享给一个服务提供商，该机构必须建立并维护管理供应商关系的策略和流程。在合同方面，这些策略和流程必须包括要求保持一个书面的协议来证明服务提供商对持有的持卡人数据的安全负责。

对准则的快速评估显示，对金融机构的供应商合同的安全性要求并不繁杂："合理"或者"合适"的安全性措施加上对数据入侵事件的公开和报告。不过，对准则和完备的风险管理的更深入解读使我们有义务做得更多。

这些保护无需增加成篇的废话，尽管法律措辞还需要不可避免地协商，曾经（特别是在遵循 PCI DDS 的时代）处理过金融机构或个人信息的供应商应该已经习惯了这些需求，而且已经有了标准的响应机制。

（作者：Andrew M. Baer, Esq. 译者：李博文 来源：TechTarget中国）

供应商风险管理：过程化和文档化

在管理供应商合同的时候，非常重要的一个环节是将过程化考虑进去。订立合同不是孤立地去承诺某种义务，而是金融机构的综合信息安全计划的重要组成部分。一个对自己机构的信息安全官存有质疑的监管者可能希望该下属持有一份保持更新状态的有关于第三方供应商以及本机构对于这些第三方供应商的风险分类的列表。这些第三方供应商拥有访问非公开的个人信息以及他们所拥有的各种类型信息的访问权限。(PCIDSS 规程（Payment Card Industry Data Security Standards,支付卡行业数据安全标准）的第 12.8 节就有类似规定，它的要求所涉及的实体应该保存一个服务提供商列表。这些实体与他们的服务提供商共享了支付卡持有者的数据。)从监管者和审计者的角度来看，为了备份本机构的供应商风险评估信息，保持一些有关于对供应商进行的严格审查或审计报表或者类似这些报表的摘要信息的文件对于达到这个目的也是很有帮助的。

在任何一次监管检查时，我们都应该能方便地提供重要的供应商合同的拷贝和具有讨论公司承包策略资格的员工名单的拷贝。不知道你的供应商或不了解你的供应商的信息，就必然导致一个不准确的、不健全的评价。为了使供应商文档的管理更容易，公司的法律部门应该使用合同管理数据库软件来追踪供应商关系以及从信息安全的角度来标记那些被视为高风险的合同，例如，这样数据库管理员就可以方便的打印出所有的、其供应商对帐户和社会安全号码具有访问权限的合同。

总而言之，随时查看重要的供应商合同是非常关键的，并且要在组织中避免长期存储合同而不定期查看的情况的发生。金融公司的法律工作者、操作人员、合规人员以及信息安全工作人员必须要知识渊博，并且当应对监管者时互相之间要保持一致。例如，如果一个公司的法律顾问将强健的审计权包含在供应商合同中，但从来不行使审计权，或者就算他们行使了审计权，信息安全执行官也无法提供文档来表明实际发生过的审计行为，那么这些行为将没有任何价值。

综上所述，缔结合同不仅仅是律师们所期望的。合同化是供应商信息安全风险管理中的至关重要的环节。当前尤其是在资金短缺的情况，我们往往奢望能以最低的价格迅速地购买到 IT 项目的解决方案，当然这也是可以理解的。然而，对于金融机构以及日益增多的非金融机构而言，结构严谨的合同也不仅仅只是律师们所要求的。而是上升到了一项必须遵守的行业义

务，成为监管机构和立法机构所关注的焦点。尽管如此，随着 IT 项目管理者，信息安全人员以及法律顾问统一意见，随着供应商越来越清晰地意识到这一问题，合同化的新焦点也不一定意味着无止尽的瓶颈和延误。

（作者：Andrew M. Baer, Esq. 译者：行久 来源：TechTarget中国）

如何防御黑客窃取信息：员工意识和风险评估策略

想想你们公司有的基础设施有多大可能正被不怀好意的黑客盯上。你的基础设施的信息具有多大的价值？是否知道你有多少敏感信息被黑客用小花招给公诸于众了？该怎样阻止黑客窃取你的信息呢？

任何一个真正的黑客的攻击总是从侦察目标开始的。让我们来看看几个比较常见的技术同时也学学如何制止黑客窃取信息。

往往网上散布着的关于你公司的敏感信息会多得让你惊讶——它们就那样等着被人发现。你是否曾经上 IT 论坛搜索你的域名？试试看！公司技术人员很可能会在公共论坛上发布问题和解答，其间会提及公司正在使用的具体设备，也许他们使用的还是他们的工作电子邮件的地址！哎哟！很显然，他们没有意识到危险：那些黑客可能不需要接触你的网络就了解了你在使用哪种类型的防火墙或服务器。

为了避免这种情况，可以开展一个员工意识和公司风险评估政策的培训，从而要求企业用户在公共论坛发布任何信息时使用非工作电子邮件地址。确保你的员工知道公司的名称不应该出现在这些贴子中。这样做并不会影响他们的问题得到解答，然而公司的基础设施的细节却不会让全世界都看到了。

为了了解你的技术人员的信息，另一个黑客会去的地方是在线 IP 地址数据库和网站登记库。 实际上，全球的这类信息被分别保存在四个数据库中。检查 ARIN.net 上的 Whois 数据库，看看在你的公司的域名列表下是否有你公司的技术人员的名字、邮箱、或是电话号码。理想的情况是，你应该只提供了公共的信息，以防止黑客猜测这些人员的身份信息，从而诱使你的员工泄露他们的密码或其他敏感信息。

一个人的垃圾是另一个人的宝藏…是有这么个谚语！“捡垃圾”是一个古老的，肮脏的，但仍效果显著的信息收集技术。攻击者通过分析你不要的信息，寻找社会安全号码，电话号码，用户 ID，IP 地址和密码。鉴于此，员工意识培训计划应得到认真地执行，以教会员工如何妥善销毁任何可能被利用的信息。您可能认为这是不必要的，但我仍然鼓励你们，特别是 IT 领域的公司，检查每一台网络打印机旁废弃文件的内容。想想如果你发现的东西到黑客手里，你会觉得放心吗？

(作者：Vernon Habersetzer 译者：Sean 来源：TechTarget中国)

外包安全服务的风险

问：我们公司想要采用外包服务，包括信息安全。对信息安全服务提供商的赞成和反对的理由是什么？有没有危险的境况导致安全不能外包呢？

答：对于这个问题，我可以写一本书出来。但是简短来说，理解你所说的“外包信息安全”的意思非常重要。我一直认为没人能因为自己有能力处理所有的事情而获得嘉奖，所以，我非常喜欢把内部资源不能真正增加价值的特定功能外包。像邮件安全或者防火墙监控等都可以外包。

但是我强烈认为企业的 信息安全项目的责任必须要在内部。安全是一个业务功能，所以安全经理（从讨论的角度来说我们把这些人称作 CSO）需要在公司现场建立可靠性，需要亲自处于循环中，并把安全的价值转达给其他主管。

我不太清楚外部的一方怎么有要求、能力或者动机来对安全负责人。最后，我相信“火的教义”。也就是说如果出现错误，谁应该被推上火刑架？我怀疑是外包提供商的团队，所以内部控制安全项目非常重要。

另一个推论是你是否会外包 CIO 呢？即使技术操作的其他不能移交给了服务提供商，你可能不会——那么你为什么会外包安全项目管理？

（作者：Mike Rothman 译者：Tina Guo 来源：TechTarget中国）

风险评估应该包括哪些步骤？

问：风险评估应该包括哪些步骤？

答：风险评估是个复杂的问题，不是几段话就可以讲清楚的，但是它是信息安全的核心。

为了保护系统，你必须决定风险的等级。风险等级越高，就越需要保护。你不想把信息安全的预算花费在保护风险等级不高的系统上，而是想在花在高风险的系统上，那些敏感的客户数据，或者例如，解决金融交易。而这好像是很平常的，很少的公司正确地对 IT 风险作了评估，最后不加选择的浪费了他们的预算和资源，而大部分的敏感 IT 资产保护的并不好，而是都用在了价值较低的信息保护上了。

概括来讲，风险评估包括对 IT 架构的三个部分的评估：威胁、漏洞和风险。例如，威胁可以是黑客获得了你的电脑信息数据库的黑客。漏洞是数据库国企了，不再有最新的安全补丁安装。所以，风险可能很高，因为系统没有补丁、网站位于没有防火墙的不受保护的网络上，而且和互联网直接连接。

这种情况在拥有经验丰富的安全人员的公司不可能出现，但是仍然证明了一个问题。因为我们知道风险很高，而且非常可能发生，我们知道我们需要减轻控制。我们已经评估了风险而且知道哪里以及如何保护我们脆弱的 IT 资产。在这种情况下，风险评估告诉我们首先给服务器打补丁，阻止防火墙端口访问服务器，并和互联网断开连接。

记住，这不仅是关于 IT 风险，以及保护服务器和 Web 网站。危险的 IT 系统最终会导致数据丢失、储运损耗和恶意使用，所有这些都会破坏业务名誉或者更糟。

更多的风险评估的信息，可以访问标准和技术的国家研究所的网站http://csrc.nist.gov。他们的电脑安全资源中心包含广泛使用并由信息安全专家推荐的的风险评估方法。

（作者：Joel Dubin 译者：Tina Guo 来源：TechTarget中国）

社交媒体：金融机构的风险管理策略

社交网络、微型博客和协作媒体（如 Facebook、LinkedIn、Twitter 和一些 wiki 网站）的增长,给金融机构和其他行业带来了挑战和机遇。和几年前出现的博客一样，社交媒体给企业提供了一个新的广告渠道以及同用户交流的渠道，可是机构内部员工博客的使用却给机构带来了名誉风险，责任风险和信息安全风险（除了丧失生产力之外）。因此金融机构需要采用全面的社交媒体战略，制定满足业务需求和公司文化需求的政策，以便于发现新媒体潜在的风险，并对其进行风险管理。

然而，金融机构却不像其他行业，因为他们在跟客户交流、为他们的产品和服务作广告、保护客户和机构本身不被欺骗、管理名誉风险方面都必须满足特别的要求。让我们看看金融机构的特殊风险管理跟社交媒体冲突的地方，以及一些可供他们选择的互联网使用政策、互联网营销政策，以及通信和品牌管理战略。

制定一个公司互联网使用政策

金融机构应该认真考虑是否允许雇员在工作的时候私自使用社交媒体。如果允许，那么就得有一个书面的互联网使用政策，每人员工都应在上面签字，而且这个政策要明确规定如果违反就会得到惩罚。这种政策中的很多基本条款跟非财政企业一样，比如：杜绝诽谤或者骚扰的内容，不涉及第三方的版权问题或者商标问题，不能涉及机密或者隐私。

不过，监管机构把名誉、业务和责任风险管理作为安全和稳固不可分割的一部分，这使得这些基本条款对于金融机构来说显得尤为重要。因此，一个财政机构的负责规则遵守和信息安全官员应该准备随身携带公司互联网使用政策的副本，并准备在监管调查时讨论它。一切非公开的个人信息和任何相关财政数据或者产品可行性数据都是机密资料，不得泄漏。跟其他行业的政策一样，除非一个社交媒体批准了沟通方式或者广告形式，否则当员工使用这个媒体谈论一些跟金融机构有关的内容时都要有一个免责声明：发表的言论只反映了员工的个人观点而不代表金融机构。

因为金融方面的规章制度在产品广告中需要具体的披露，这种情况同样会受到以不公平和欺骗的名义进行的详细调查，所以金融机构除了需要一个免责声明之外，还应该禁止员工用博

客或者社交媒体对产品和服务的有关条款、特点或者可用性进行描述或者评论，包括定价、费用、酬劳、资格或者决策标准等。这些方面的信息交流必须通过官方渠道。

一个金融机构应该还要考虑是否采取进一步行动，禁止对本机构业务的一般性评论，因为某些评论可能错误的反映了机构的安全和稳固或者名誉（举个例子，“我在某信用卡部门工作，我最近发现许多违规操作”）或者可能误导或欺骗别人。如果允许进行一些评论，员工则应该明确说明她或者他跟金融机构的从属关系，还要包括一份免责声明：这些言论只代表他或她的个人观点。

市场营销和客户信息交流政策

除了考虑是否允许员工私人使用社交媒体和允许到什么程度之外，金融机构应该把社交媒体纳入到他们的营销策略和跟用户信息交流的政策中，因为快速和广泛使用的社交媒体会已经成为了一个强有力的交流渠道。这样做的危险是：社交媒体（尤其是 Twitter）的非正式性会导致自发的、不受系统程序规范和控制的社交媒体的使用，越过那些在书面邮件、电子邮件和其他的营销与信息交流渠道之前必须通过的法律法规审查。

然而，正是因为社交媒体是另一种信息交流渠道，以保护消费者为重的监管机构很可能会对其用同样的规则标准。所以，在媒体发布的所有信息中，如果有关于金融机构自身业务（比如，一个 Facebook 网页），则应该经过同样的审查流程。如果公司上市的话，还应包括安全规则的合法性审查。包括金融机构产品或服务的条款、特点或者可用性的描述或说明（包括定价、费用、酬劳、可行性或者决策标准等），应该首先接受遵从标准的审查。（这可能限制在 Twitter 上对一些具体的产品做广告，因为任何免责声明都可能会超过公告所规定的 140 个字符上限。）

如果社交媒体用于个人之间的信息沟通交流，还会有其他的规则标准、信息安全和品牌管理方面的事宜。因此，开发的脚本、准则和程序应该能够处理这种用户沟通形式，让这种形式跟电话和电子邮件沟通成为一体，并能解决后续的问题。

受监管的金融机构一般需要保留跟用户信息交流文档的副本，可能会包括 Twitter 消息和 Facebook 评论，所以如果有一个可以捕获这些信息的系统，就能实现信息与用户的帐户记录的联系。那样说的话，社交媒体就不应该用来接受或者处理个人信息和个人事宜；金融机构应该通过插入显著信息和发布警告用户的公告清楚地重复提醒用户金融机构从不要求获取这样的

信息，也不会接受社交媒体上传输的数据。用户应该学会脱机处理个人事宜。这对保护机构不会遭受盗窃来说是一个关键，这样做还能保护金融机构免于网上钓鱼和电子欺诈，避免损失。

品牌管理和商标保护

为了打击骗子利用社交媒体，仿冒金融机构商标的名字、形状来进行诈骗，金融机构必须切实加强管理商标的策略。这个策略要与该机构的信息安全策略、域名及商标保护战略相协调，还应该包括一个机构内部资源的使用或者商标监视服务，以便于在社交媒体网站和互联网的其它地方侦查潜在的、有害的或者非法使用机构标志的侵权行为。

由于Facebook最近添加的新功能，允许用户注册包含域名url的用户名（例如，www.facebook.com/你的名字），人们开心担心“名字侵权”（恶意抢注）。在开始注册的前一个星期里，Facebook允许联邦注册商标的拥有者提交一个在线表格来阻止别人用他们的商标注册用户名，但是现在这个提交程序关闭了。没有了阻止，很简单，金融机构如果不能“先到先得”（比如，在其他人注册之前在社交媒体网站注册自己的商标作为用户名），就无法得到这个域名。金融机构应该立即去注册，即使他们需要时间来考虑怎么去构建内容或者开发一个社交媒体政策。

当一个企业遇到恶意侵权的时候有这么一些保护措施。举个例子，Facebook 和 Twitter 的应用条款中，包含了各种各样的规定，清楚的禁止侵害第三方商标和冒充其他用户，两个网站都保留了收回用户名的权利（Twitter 规定，如果一个用户名侵犯了一个合法用户的商标权，Twitter 有权收回这个用户名）。Facebook 也提供了一个在线表格，商标拥有者可以通过这个提交申诉。当一个侵权者使用别人的商标明显是欺诈或者损害了公共利益时，比如网络诈骗，社交媒体网站会作出反应，并和相关方进行合作。然而，当某用户名使用了仅存在微妙差别的商标并进行公正地使用时，这种争端就不好处理了。

和域名恶意侵权（恶意抢注）不同的是，在联邦商标法令和 ICANN 统一域名争端解决政策中都有补救措施，这些法令法规跟域名注册协议组成了一个整体。而社交媒体中侵权方面的法律还处于起步阶段。如果跟社交媒体网站合作并不能减轻不良影响，又能确定侵权者是谁，那么就商标侵权和/或者不实的来源标志提起民事起诉是一个可行的办法，前提是有证据证明侵权者用金融机构的名字或者商标进行商业活动（比如获得钱财或者信息，或者引导用户去访问另一个提供竞争服务的主页或者网页），从而可能给消费者造成困惑或者欺骗。如果一个商标非常著名，侵权者拿它来进行非法商业活动会削弱或损害它的影响力，或者让它名誉受损，对此同样也可以提起商标淡化（trademark dilution）诉讼。

谨慎行事

作为高度自律的、对公众有特殊责任的企业，金融机构必须在引起骗子、监管人员和起诉律师的注意之前学会管理社交媒体的风险。如果有一个正确合理的社交媒体政策，金融机构就可以从一个全新的、充满活力的交流渠道中获利，同时又能避免对他们的安全、稳固和底线构成的威胁。

(作者：Andrew M. Baer, Esq. 译者：Sean 来源：TechTarget中国)