会化媒体环境中，企业如何应对社会化媒体带来的各
全威胁？本书给予了系统、全面的解答，并提供相关
用解决方案。

Mc Graw Hill Education


# 社会化媒体与企业安全

## 社会化媒体的安全威胁与应对策略

（美） Gary Bahadur Jason Inasi Alex de Carvalho 著

姚军 等译

机械工业出版社
China Machine Press

# SECURING THE CLICKS

Network Security in the Age of Social Media

# 社会化媒体与企业安全

## 社会化媒体的安全威胁与应对策略

（美） Gary Bahadur Jason Inasi Alex de Carvalho 著

姚军 等译

机械工业出版社
China Machine Press

水能载舟，亦能覆舟，社会化媒体在给企业带来机遇和价值的同时，也给企业带来了潜在的威胁。本书通过生动的实例、专家的经验，讲述了在新的社会化媒体中，企业如何建立起一套行之有效的社会化媒体安全策略。书中以一家虚构的公司为例，根据成熟的安全模型，从人力资源、资源利用、财务、运营和声誉五大部分，概述了企业在社会化媒体时代可能面临的安全威胁和相应的对策，不仅提供了社会化媒体使用管理、危机管理、声誉管理中的理论指导，而且提供了许多具有极高操作性的实用管理方法以及软件工具，帮助企业打造安全的网络防御能力，并能够通过模型不断扩展更新自身的安全防御手段。

本书按照实施社会化媒体安全框架的过程分为五个部分。第一部分：评估社会化媒体安全，主要介绍了如何确定企业环境中与社会化媒体使用相关的情况。第二部分：评估社会化媒体威胁，深入分析威胁对机构的影响。第三部分：运营、策略和过程，介绍了如何控制组织中社会化媒体的使用方式。第四部分：监控和报告，介绍如何实现监控和报告公司社会化媒体活动（内部和外部）的工具和技术。第五部分：社会化媒体 3.0，汇总了本书的主要知识，以及如何实现本书概述的流程，开发评估机构对社会化媒体利用情况的安全战略。

本书适合一般公司的全体人员阅读，特别是信息技术、人力资源（HR）、市场、销售主管，以及其他管理人员等。



**本书版权登记号：图字：01-2012-1014**

**图书在版编目（CIP）数据**

社会化媒体与企业安全：社会化媒体的安全威胁与应对策略 /（美）加里（Bahadur, G.）等著；姚军等译 . —北京：机械工业出版社，2012.7
（信息安全技术丛书）
书名原文：Securing the Clicks Network Security in the Age of Social Media

ISBN 978-7-111-39038-1

I. 社… II. ①加… ②姚… III. 传播媒介－影响－企业安全－研究 IV. X931

中国版本图书馆 CIP 数据核字（2012）第 146315 号

机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码　100037）
责任编辑：秦　健
北京市荣盛彩色印刷有限公司印刷
2012 年 8 月第 1 版第 1 次印刷
186mm×240mm • 14.5 印张
标准书号：ISBN 978-7-111-39038-1
定价：59.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991；88361066
购书热线：（010）68326294；88379649；68995259
投稿热线：（010）88379604
读者信箱：hzjsj@hzbook.com

# 译 者 序

互联网彻底改变了人们的生活方式，在它的基础上，一次又一次的革新颠覆了人们看待世界的眼光，不断地为我们带来惊喜，同时也悄悄地带来了许多隐患。

社会化网络是近年来非常流行的新生事物，它的迅猛发展正如当年万维网的出现一样，为人们的生活打开了一扇新的大门，使人们之间的距离变得更近，交流更加顺畅，地球因此越来越像一个大型社区，这为人们的生活增添色彩，为各种企业带来了更多的商机。

任何新生事物都有其两面性。人们沉浸在资料共享的快乐之中，享受一切尽在指尖之下的满足的时候，威胁也随之产生。快速传播的资料为企业间谍活动、针对个人和企业的声誉攻击、身份盗窃、社会化工程攻击等带来了便利，不管是企业还是个人，不管是否使用社会化媒体，都可能卷入这场风暴中。本书揭示的一个个发人深省的案例，使我们不得不重新审视这个世界，在新的社会化风暴中，大型公司可能因为员工的疏忽大意、不怀好意的竞争者或者犯罪分子发动的误导性宣传而失去几十年苦心经营的企业形象，而普通的人们也可能因为在数据交换中的不慎而招致解雇、诉讼甚至生命危险。没有人能够活在世外桃源，世界已经改变，我们唯有积极地去了解新的机会和挑战，并且学会保护自己和运用新工具的方法。

本书通过生动的实例、专家的经验，讲述了在新的社会化媒体圈中，企业如何建立起一套行之有效的社会化媒体安全策略。本书以一个虚构的公司为例，根据成熟的安全模型，从人力资源、资源利用、财务、运营和声誉五大部分，概述了企业在社会化媒体安全中各个方面的威胁和对策，不仅提供了社会化媒体使用管理、危机管理、声誉管理中的理论指导，而且提供了许多具有很高操作性的实用管理方法以及软件工具。通过对本书的认真研习，在6个月甚至更短的时间内，一家原本毫无防备的企业就可能打造一定的防御能力，并能够通过模型不断扩展更新自身的安全防御手段。

在本书的翻译过程中，我们深深感受到现代社会化媒体中令人震惊的潜在威胁，也为我们能够在遭受攻击之前就掌握这些知识而深感幸运。相信这本书能够为许多企业的安全团队提供专业级的指导，从而避免案例研究中那些灾难性的事件。

本书的翻译主要由姚军完成，徐锋、陈绍继、郑端、吴兰陟、施游、林起浪、刘建林、陈志勇等人也为本书的翻译工作作出了贡献，在此也要感谢机械工业出版社的编辑对翻译工作提出的许多中肯的意见，同时期待着广大读者朋友的批评指正。

# 序　言

就在你再次觉得使用互联网是安全的时候，输入“添加 technorati 标签”命令造就了一个实体世界和虚拟世界之间的全新接口。不管你称它为社会化媒体、社会化网络或者一些还不流行的术语如“团体思维”（哦，等等，是这么叫的吧？），这种现象都实际存在，并且已经深深地进入了我们的日常生活中。

遗憾的是，和许多之前的适应辐射一样（想想 .com），更多网页曝光的技术和欲望总是先于控制局面的愿望或者能力而出现。正如本书的作者在第 1 章中引用的那样，“纽约法院最近对社会化媒体网站（如 Facebook 和 MySpace）提起的用户隐私权合理要求诉讼只是一相情愿的想法”。作为长期（并且仍然在积极实践）从事安全工作的专业人士，我可以证明，这可能是对这个仍然年轻的世纪最大的低估。

对于咨询安全信息的客户，我问的第一个问题总是“你要保护的是什么？”这个问题严格定义了在保护资产安全中的投资水平和类型。社会化媒体的设计专注于利用我们最宝贵的资产——我们的本质、我们的位置（“存在”）、我们的合作者、我们的日常活动和习惯、我们的名誉或品牌，甚至我们通过 Twitter 每次用 140 个字符表达的重要想法。你愿意投资多少来保护组成你的一切信息？

从更实际的角度看，人是社会性的动物。历史上，我们在 Facebook 之前就分享了许多有关自己的信息。（记得浏览当地的电话簿吗？姓名、号码、地址……）不管我们天真与否，谈到信息交换，都能接受风险－收益相当的平衡：我们得到的比付出的多，对吗？毫不奇怪，互联网在很大的程度上完全依赖于这个风险－收益命题：免费得到巨大的价值（Wikipedia、YouTube、Farmville），全都是用于了解你，并且将你介绍给商业买家交换得来的。不管你是否喜欢，我们都身处这一框架之中。

所以，如果你正在寻求更安全的社会化媒体体验，你将要发动的是一场艰难的战役，对手可能是人类的革新潮流本身。幸运的是，你已经做出了一个很好的选择——寻求本书作者的忠告（我已经在信息安全领域与他们共事了很长时间）。本书收集了许多宝贵的内幕信息、技巧、战略和战术，这些信息曾经帮助世界最知名的公司安稳地渡过社会化媒体的狂暴之海。从策略到人员配备、预算到战略规划、技术调查到 PR 响应，本书覆盖了所有这些基础知识，以及在当今技术趋势下，任何商业人士所面临的高级问题。开始阅读吧，自信地大踏步跨进这个美好的新社会化世界！

Joel Scambray
Consciere 公司 CEO
《黑客大曝光：网络安全机密与解决方案》
《黑客大曝光：Web 应用程序安全（原书第 3 版）》[⊖]和《黑客曝光：Windows 安全》作者

⊖ 本书中文版已由机械工业出版社引进出版，ISBN：978-7-111-35662-2。

# 前　言

## 为什么创作本书

互联网是人类文明史上发展最快的媒体。随着时间推移，它的采用率和延伸范围已经远远超过了电视和广播。20 世纪 90 年代预示了人类通信的新时代，从更广泛的意义上说，这重塑了我们对世界的看法。这个新世界也开启了隐私和公司安全问题的潘多拉魔盒。由敏感数据、内部通信或者员工行为习惯的泄露引起的破坏是对当今世界上所有公司的真正威胁。

由于互联网的使用变得普遍，越来越多的人和员工通过容易使用和大量散布的社会化媒体技术发表自己未经过滤的言论和体验。对于任何能够访问互联网的计算机或者设备的人，以及世界各地的无数业余爱好者和痴迷者来说，这些技术使发布未经编辑的文本和媒体变得非常简单。人们可以使用免费使用的软件工具创建各种类型的媒体，匿名地张贴这些内容。有线和无线的网络通过社会化媒体平台连接，现在出现了仅用 140 个字符建立或者破坏一个品牌的能力。

本书是一本实用指南，有助于公司保护自身利益、资产和品牌免遭社会化媒体风险，保护数字资产和声誉免遭使用社会化媒体平台的攻击者危害，同时通过安全使用社会化媒体工具和平台与内外部社区沟通。目前许多书籍都论及利用社会化媒体的方法，但是大部分是从企业销售或者客户服务以及个人品牌着眼，我们希望培养客户正确地加固社会化媒体使用、免费共享或者提供信息和企业资源的安全。

社会化媒体已经进入了我们生活的各个方面。仅仅 Twitter 从 2009 年 2 月开始每年就增长 1382%。Facebook 拥有超过 7.5 亿成员，其中包括 1 亿移动用户，并且还在增长。Skype 的用户已经超过 6 亿。你所生活的本地社区现在可以从全球进行访问，你可以与住在印度的人谈话，就像和你对门的邻居谈话一样。我们所愿意共享的自身信息——工作、家庭和活动扩展了我们的社会化网络，但是也使侵犯隐私权、身份盗窃、信息滥用和泄露、版权侵犯和商标侵权变得更容易，导致公司资产和声誉受损。

通过定义公司利益的边界，即使在反映负面的客户体验时，也能推进安全和富有成效的对话。风险可以最小化，并且安排业务流程来处理开放沟通可能发生的不测事件。随着全世界都在学习社会化媒体的使用方式，公司、员工、个人和社会化媒体平台本身也会不断变得更加成熟。本书将帮助公司安全地进行这一发现之旅。

## 本书读者对象

我们的主要焦点是公司和对公司资产的挑战。本书聚焦于公司全体人员——信息技术、人力资源（HR）、市场、销售主管，以及其他管理人员和员工本身。HR 主管可能需要编写公司安全策略的指南。IT 主管可能需要指导，了解使用何种工具可以加强不断变化的社会化媒体环境安全指南。市场主管需要发起营销活动，但是必须以保护品牌声誉的方式安全地进行。管理

层可能有暴露公司黑暗面的个人社会化媒体出口。

员工可以获得许多方面的领悟：如何在工作场合以及为公司正确使用和利用社会化媒体，如果不正确地使用社会化媒体，社会媒体如何危害自身以及对公司带来负面影响。员工必须理解，在使用社会化媒体时如何才不会破坏公司的声誉，以及如何避免法律问题，例如，避免公司品牌侵权。

本书的另一部分读者是小企业主和员工。大企业所适用的课程也可以在中小型企业（small and medium-sized business，SMB）市场上使用。在 SMB 中，员工比大企业中更不容易控制；因此，社会化媒体的不正当使用情况更多。SMB 可以使用本书作为路标，形成成本效益高和安全的社会化媒体战略，而不需要雇用外部顾问实施高成本的战略。

## 如何使用本书

企业和专业人士监控那些提及他们的产品、品牌、服务和关键员工的在线谈话面临着挑战，这些监控活动旨在理解客户意见、识别商标侵权和品牌侵权，以及理解业界和竞争形势。在确定某个人的影响，以及那些人言论的影响时，企业面对着更多的挑战。顺着这一链条，与社会化媒体相关的进一步挑战包括：

- 创建合适的战略以应对各种固有风险。
- 分配适量的资源以计划、维护和调整具体措施。
- 开发企业范围内的社会化媒体策略。
- 从企业内部和社区内雇用、培训和发展社区管理人员。
- 确定社会化媒体各种目标相关的衡量标准和性能量度，包括风险降低目标。
- 在数据移动和跟踪控制中实现安全控制，并监控可能通过社会化媒体渠道发生的数据丢失。

大部分章节以一个案例研究开始——公司面对社会化媒体挑战的一个实用的真实示例。我们在每一章中提供：实用的解决方案，实现自己的战略的步骤，以及可以用于管理社会化媒体安全战略的检查列表、工具和资源。在我们的网站 www.securesocialmedia.com 上可以获得策略模板和不断变化的社会化媒体的重要更新。

### 什么是 H.U.M.O.R. 矩阵

社会化媒体的影响可以在整个机构中感觉到，并常常向常规的操作规程发起挑战。为了做好安全参与社会化媒体平台的准备，你需要一个评估和处理需要改进领域的框架。本书介绍一套灵活的部署、管理社会化媒体战略并加强其安全的方法论。H.U.M.O.R. 矩阵提供了从机构的人力资源（Human resource）、资源利用（Utilization of resource）、财务支出（Monetary spending）、运营管理（Operations management）、声誉管理（Reputation management）出发，评估、处理、控制和监控社会化媒体的基础。

# 本书组织结构

我们已经开发了一个安全框架，你可以按照评估过程开发一个处理社会化风险计划，以及控制和监控社会化媒体使用的实际方法。本书按照实施社会化媒体安全框架的过程分为 5 个部分：

**第一部分：评估社会化媒体安全。**这一部分介绍在企业环境中与社会化媒体使用相关的情况。这个部分里概述了评估当前环境的战略。第 1 章定义评估整体社会化媒体形象的过程。首先，你必须理解管理公司的方式、业界的做法和竞争者的做法。第 2 章详细定义 H.U.MO.R. 矩阵过程。详细说明了矩阵的每个部分，并提供了将企业当前的挑战融入一个具体框架的步骤。在第 3 章中，根据客户、竞争者和员工对公司的意见完成环境评估。你对有关公司的所有议论的洞悉，为理解你所面对的威胁和管理你的社会化媒体局势所需的控制方法打下了基础。

**第二部分：评估社会化媒体威胁。**这一部分介绍如何确定威胁对机构的影响。第 4 章概述识别社会化媒体威胁的过程。你必须评估来自员工、客户和竞争者的威胁，并理解不断变化的威胁形势。第 5 章带你经历邪恶的人采用、启动和关联威胁的过程。威胁可以针对个人或者公司，你应该理解可能导致攻击的不同威胁方向。

**第三部分：运营、策略和过程。**这一部分阐释了如何控制组织中社会化媒体的使用方式。第 6 章描述了应对社会化媒体使用威胁所必需的社会化媒体安全策略。我们为安全使用社会化媒体定义了最佳的战略，因此你可以决定如何开发用于社会化媒体的有效安全策略和规程。

接下来的章节——第 7 ～ 11 章，为 H.U.M.O.R. 矩阵的每个部分开发可操作的策略和规程。它们为你提供处理（现在和将来的）威胁以及社会化媒体战略所必需的实施指南。

**第四部分：监控和报告。**这一部分介绍如何实现监控和报告公司社会化媒体活动（内部和外部）的工具和技术。每章对应 H.U.M.O.R. 矩阵的一个部分，定义了随时维护安全基础架构所需要采取的具体措施。随着社会化媒体平台的改变，你的过程要能够适应新的技术和服务。

第五部分：社会化媒体 3.0。第 17 章分析了你已经学习的知识，以及如何实现本书概述的流程，开发评估机构对社会化媒体利用情况的安全战略。在第 18 章中，我们开始为所预见的社会化媒体的未来以及造成的社会化媒体安全挑战做预先的规划。附录收集了本书中介绍的所有工具和社会化媒体资源。

> **注意** 我们还在 www.securingsocialmedia.com 网站上提供了支持信息和本书讨论的相关工具的链接。请经常关注这个网站，以得到更新和新工具，这些工具可以帮助改进你的社会化媒体安全，我们在它们可用时进行审核。

读完本书之后，你将拥有实用的方法，将公司的社会化媒体使用变成更加安全和全面的过程。使用本书讨论的这些工具、提供的策略文档以及渐进式的 H.U.M.O.R. 矩阵框架，你将不会再被社会化媒体的风险所吓倒。

谢谢。

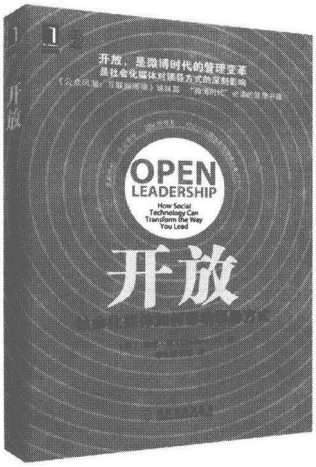
Gary、Jason 和 Alex

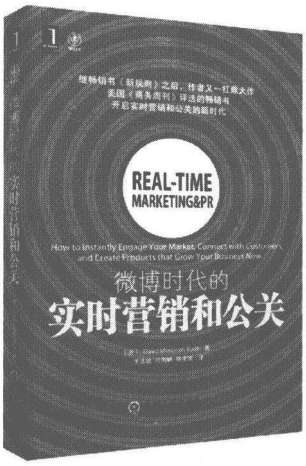
HZ BOOKS
华章科技

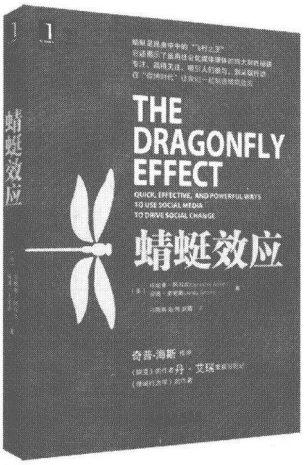
Social Media Time

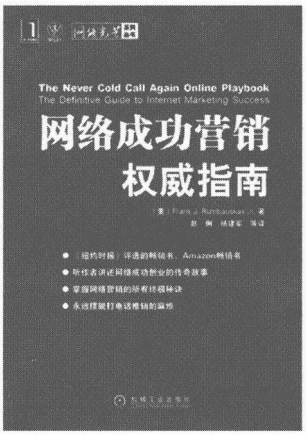
# 新媒体时代

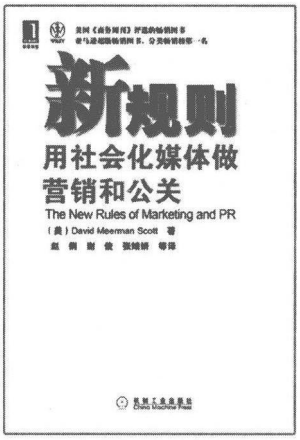
## 营销、公关、管理第一品牌图书



# 目　录

## 第三部分 运营、策略和过程

## 第四部分 监控与报告

## 第五部分 社会化媒体 3.0

# 第一部分

# 评估社会化媒体安全

# 第 1 章

# 社会化媒体安全过程

社会化媒体安全从理解组织的环境以及由于这种新的沟通媒介给公司带来的全球性挑战开始。社会化媒体的使用已经将公司暴露到新的挑战面前。信息技术（IT）部门必须发展，更加贴近市场、人力资源、法律、财务和运营，以实施减少社会化媒体风险的战术手段。

本章为评估在你的组织中由客户以及竞争者使用社会化媒体的固有风险做铺垫。你将学习如何：

- 确定分析行业好坏做法的方法。
- 评估现有社会化媒体安全过程，确定当前使用不同工具、网站和业务过程中的漏洞。
- 从员工使用、客户交互和竞争形势等方面度量社会化媒体对你的组织造成的影响，以及业界对减少所遇到的整体风险所做的努力。

## 1.1 案例研究：由无准备的社会化媒体策略引起的声誉损失

没有实施管理社会化媒体风险的公司很容易在品牌和财务盈亏底线上遭到攻击。在 2010 年夏天，由于深海钻井平台爆炸引起原油持续涌入墨西哥湾，石油巨人英国石油公司（BP）面临严重的危机。在 107 天中，该公司努力遏制原油流入大海，并发动了一场公关活动来应对这一危机。公司发言人通报了该公司为清除原油所做的努力，以及为该地区提供的 200 亿美元恢复基金。但是，BP 对于网上的负面言论无计可施，无数的人在 Twitter 和博客上发布表达忧虑的帖子，并且在 Facebook 上组成了抗议组织。他们不仅担心浮油对环境、当地捕鱼业以及旅游业的影响，而且对 BP 缺乏透明度表示反感。BP 的 CEO 托尼·海瓦德越来越被网上评论为敷衍、草率，有时甚至是冷漠的。

该公司严格控制媒体进入浮油区，禁止清理人员穿戴保护装置。BP 自己的社会化媒体出口只有不到 18 000 个追随者，而盛怒的市民们创建的一个 Twitter 账户（BPglobalPR）在几周内就有了 15 万以上的追随者。@BPglobalPR 这个 Twitter 账户通过销售 T 恤和其他商品筹集了超过 1 万美元。

### 哪里出了问题

BP 对社会化媒体社区的利用和反应说明，该公司在许多领域内没有应对公司和品牌所面临威胁的流程。BP 在墨西哥湾的钻井平台爆炸可能是没有人曾经预测过的不可预见事件。该公

司的操作规程应该能够避免这种泄漏，但是这超出了本书的讨论范围。

但是，该公司应该很好地预计到社会化媒体对泄漏或者任何大型石油事故的反应。很明显，人们将会通过在网上发布表达忧虑和愤怒的帖子，对这种事件做出公开的反应。BP 应该有应对这种事故可能结果的计划，制订应对社会化媒体后果以及公司声誉和财产的特定攻击的安全措施。

从人力资源来讲，该公司应该雇用在线社区管理人员监督其社会化媒体形象。但是，该公司仅仅通过 PR 部门准备的信息做出反应。结果是，该公司的官方 Twitter 账户 @BP_America 在本书编写时只有 18 000 个追随者，而对 BP 的努力进行嘲讽的虚拟账户 @BPGlobalPR，很快就有了高出许多倍的追随者——最后一次统计时大约有 179 000 人。

从公司**资产**的利用上说，BP 的绿色标志被网民们“重新混色”，以反映原油对环境的影响，例如 @BPGlobalPR 账户使用了全黑的标志——从该标志上漏下一滴石油。在 Flickr 和 Facebook 上还贴出了许多其他重新混色的标志，其中一些印在 T 恤上出售。该公司没有保护商标和标志的计划，也不理解这些商标和标志在工业事故中可能被不正当地使用。

从**财务方面的考虑上**说，有关 BP 的大量负面言论导致了许多糟糕的报道，最终影响该公司的价值。随着原油流入海湾，公众的愤怒情绪升高，投资者的信心随之下降。BP 的市值严重下降，导致其可能成为竞争的石油巨人的收购目标。

从**运营上讲**，BP 的一些措施在社会化媒体和报刊中遭到了大量的批评。有报道称，BP 阻止记者和摄影师接近浮油或者从上空飞过。其他有关清理工作人员的报道没有过多的遮掩，所以他们的照片没有过多的负面影响。BP 的一些关键性的商业决策无法很好地做出解释，也遭到了很多批评。这些政策包括使用分散剂——这也会破坏环境，没有采用封井设备，没有准备减压井。尽管泄漏本身无法预见，但是新闻媒体对公司前前后后所采取的行动的反应却是完全可以预见的。

从**声誉**的角度上说，网上对该公司的评论大部分是负面的。报刊报道了网民们的反应，从而将这些评论带到了传统的媒体。人们对工业事件感到不安；了解了这一点，公司应该更加诚恳地承认事实，建立亲善的关系，以及建立和网上的消费者更公开的沟通渠道。

在这 5 个关键的经营领域——人力资源、资产利用、财务开支、运营和声誉方面，BP 都可以实施许多策略，我们在本书中将对这些策略做出清晰的定义。

## 1.2　近期安全性的变化

过去，公司关心黑客的邪恶行为和公司间谍活动。一个相对小但是具有高度技巧的集团可能代表着对任何规模公司运作的主要威胁。现在，任何连接到互联网，并且怀有私心的人都可能对最受喜爱的品牌造成不可弥补的破坏。公司面对的攻击类型已经从纯粹的技术黑客攻击发展为对品牌形象和公司声誉的攻击，已经有很多公司受到了这种伤害，包括 Gap（公众对新标志的嘲笑）、西南航空公司（演员 / 导演凯文 · 史密斯因为过分肥胖而被赶下飞机，由此引发了

强烈抗议）以及雀巢公司（绿色和平组织的网上攻击，抗议其收集橄榄油砍伐森林导致环境破坏）。现在的公司似乎都无法逃脱个人发出的威胁，更不要说公众加入的联网群体。

随着社会化媒体影响的增长，安全问题越来越成为公司及其活跃的网上顾客和社区共同关心的问题。最普遍的社会化媒体安全关注点是对隐私权的侵犯和身份盗窃。纽约法院最近对社会化媒体网站如 Facebook 和 MySpace 提起的用户隐私权合理要求诉讼只是一相情愿的想法。

注意 你可以在 Traverse Legal 网站上看到更多有关诉讼、隐私和社会化网站张贴材料有效性的内容。请浏览 http://tcattorney.typepad.com/digital_millennium_copyri/2010/10/breach-of-privacy-across-social-media-sites-addressed-by-two-courtrulings-in-new-york-and-californi.html。

如果有人通过社会化媒体渠道窃取你的员工身份，他就可以使用偷来的凭证闯入你的公司。如果攻击者能够通过 Firesheep（后面还有更多论述）这样的应用程序截获员工在 Facebook 上使用的密码，这位员工在不同网站上使用相同密码的概率很大——包括你的公司网络。很容易找到一个人的姓名和关键信息——如生日、学校名称或者孩子的姓名，而许多人用这些信息作为密码的基础。随着越来越多的公司在社会化网络上出现和活跃，对个人的爆炸性攻击现在已经提升到公司级的攻击。第 4 章将会讨论，通过社会化媒体渠道传出的威胁正在变得更加复杂，没有好的社会化媒体安全策略的公司将和没有 IT 安全策略的公司一样容易遭到攻击。

## 1.3 评估流程

实施战略性的社会化媒体安全措施的第一步包括规划当前的环境，以理解加入在线社区的短期、中期和长期后果。一旦开始，公司与其开发的在线社区之间的联系就会随着时间改变，风险和挑战也随之改变。为了准备这一旅程，公司必须进行各种审核，更确切地说，是所谓的**社会化媒体评估流程**。

我们已经定义的流程对曾经管理过安全审计或者进行过安全评估的人来说似乎很熟悉。本书将按照如下的步骤展开：

1）**战略分析**，定义目前已经确定的社会化媒体战略和工具以及使用的情况，并确定所使用的社会化媒体安全措施。评估整个环境并确定漏洞所在。

2）**威胁分析**，定义和总结威胁形势并确定切入点。威胁形势指的是公司可能遭到的不同方法的攻击，不管这是使用 Facebook 应用中的间谍软件或者使用特洛伊木马应用进行的技术型攻击，还是客户在 Twitter 上对你的品牌的攻击。

3）**操作、策略和控制**，定义和实施可操作性的战术以处理威胁。实施新的策略和控制来降低风险。

4）**监控和报告**，实施一个生命期过程，用于持续监控和报告你所实施的社会化媒体工具、项目和战略以及对安全性的影响。执行一致的报告以确保新的安全策略保持有效，并且