

<<社会化媒体与企业安全>>

图书基本信息

书名：<<社会化媒体与企业安全>>

13位ISBN编号：9787111390381

10位ISBN编号：7111390385

出版时间：2012-8

出版时间：机械工业出版社

作者：（美）加里 等著，姚军 等译

页数：219

译者：姚军

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<社会化媒体与企业安全>>

### 内容概要

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。

Gary Bahadur、Jason

Inasi、Alex de

Carvalho所著的《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》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。

《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》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。

《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》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。

## <<社会化媒体与企业安全>>

### 作者简介

KRAA

Security公司CEO，资深信息安全技术专家。

针对应用安全、网络安全、社会化媒体安全、操作系统安全等领域提供预防策略和咨询服务。

曾是Foundstone公司的共同创办人之一和CIO，为《财富》500强企业提供客户管理、咨询管理、业务开发、公司战略开发、客户管理、信息系统开发等服务。

曾住美国银行高级副总裁，负责全球威胁管理，是提供风险缓解战略的推进者。

# <<社会化媒体与企业安全>>

## 书籍目录

译者序

序言

前言

### 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

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

1.2 近期安全性的变化

1.3 评估流程

1.4 组织分析：你所在行业在互联网上的好与坏

1.4.1 分析你的社会化媒体倡议

1.4.2 分析现有的内部过程

1.4.3 加强客户数据安全

1.4.4 加强沟通渠道安全

1.4.5 识别目前公司使用社会化媒体的方式中存在的安全漏洞

1.5 竞争分析

1.6 小结

#### 第2章 安全战略分析：安全策略的基础

2.1 案例研究：黑客入侵是一种机会均等的游戏

2.2 H.U.M.O.R.矩阵

2.3 人力资源

2.3.1 评估当前的环境

2.3.2 度量当前状态：H.U.M.O.R.矩阵

2.4 资源和资源利用

2.4.1 评估当前环境

2.4.2 度量当前状态：H.U.M.O.R.矩阵

2.5 财务考虑

2.5.1 评估当前环境

2.5.2 度量当前状态：H.U.M.O.R.矩阵

2.6 运营管理

2.6.1 评估当前环境

2.6.2 度量当前状态：H.U.M.O.R.矩阵

2.7 声誉管理

2.7.1 评估当前环境

2.7.2 度量当前状态：H.U.M.O.R.矩阵

2.8 小结

#### 第3章 监控社会化媒体局势

3.1 案例研究：危险的公众

3.2 你的客户和普通大众在说些什么

3.2.1 监控的内容

3.2.2 何时投入资源与负面的评论抗争

3.2.3 跟踪对话导致攻击的过程

3.3 你的员工在说些什么

3.4 “如果...怎样”场景

3.5 小结

### 第二部分 评估社会化媒体威胁

## <<社会化媒体与企业安全>>

### 第4章 威胁评估

#### 4.1 案例研究：政治性的黑客入侵

#### 4.2 变化中的威胁局势

#### 4.3 识别威胁

##### 4.3.1 攻击者

##### 4.3.2 威胁向量

#### 4.4 威胁评估和威胁管理生命期

##### 4.4.1 识别和评估

##### 4.4.2 分析

##### 4.4.3 执行

##### 4.4.4 威胁管理实战

#### 4.5 H.U.M.O.R.威胁评估

##### 4.5.1 人力资源威胁

##### 4.5.2 资源利用威胁

##### 4.5.3 财务威胁

##### 4.5.4 运营威胁

##### 4.5.5 声誉威胁

#### 4.6 评估损失

#### 4.7 开发响应

#### 4.8 小结

### 第5章 哪里有可能出问题

#### 5.1 案例研究：Firesheep-社会化媒体入侵的真实示例

#### 5.2 社会化网络特有的危险

#### 5.3 网络骚扰

#### 5.4 验证最终用户

#### 5.5 数据抓取

#### 5.6 小结

### 第三部分 运营、策略和过程

### 第6章 社会化媒体安全策略最佳实践

#### 6.1 案例研究：社会化媒体策略使用的发展

#### 6.2 什么是有效的社会化媒体安全策略

##### 6.2.1 规章和法律要求

##### 6.2.2 管理内部（自行部署的）应用程序

##### 6.2.3 管理外部应用

##### 6.2.4 企业范围协调

##### 6.2.5 行为准则和可接受的使用

##### 6.2.6 角色和职责：社区管理员

##### 6.2.7 教育和培训

##### 6.2.8 策略管理

#### 6.3 H.U.M.O.R.指导方针

#### 6.4 开发你的社会化媒体安全策略

##### 6.4.1 策略团队

##### 6.4.2 确定策略响应

#### 6.5 简单的社会化媒体安全策略

#### 6.6 小结

### 第7章 人力资源：战略与协作

#### 7.1 案例研究：“昂贵的镇纸”被解雇

## <<社会化媒体与企业安全>>

7.2 确定业务过程、规章和法律需求

7.3 社区管理员：定义和执行

7.3.1 小型公司的人力资源挑战

7.3.2 中型公司的人力资源挑战

7.3.3 大型公司的人力资源挑战

7.4 培训

7.4.1 培训社区管理员

7.4.2 培训员工

7.5 小结

第8章 资源利用：战略与协作

8.1 案例研究：不恰当的Tweet

8.2 安全过程如何处理

8.2.1 安全的合作

8.2.2 利用技术

8.3 预防数据丢失

8.4 员工教育

8.5 小结

第9章 财务考虑：战略与协作

9.1 案例研究：计算数据丢失的成本

9.2 实施控制的成本

9.3 威胁的损失及对策的成本

9.4 小结

第10章 运营管理：战略与协作

10.1 案例研究：军队的网络简档

10.2 运营管理战略

10.2.1 角色和职责

10.2.2 资产管理

10.2.3 安全意识培训

10.2.4 实体安全性

10.2.5 传达

10.2.6 网络管理

10.2.7 访问控制

10.2.8 应用程序开发与测试

10.2.9 符合性

10.3 控制手段的审核

10.3.1 内部安全工具和社会化媒体网站审核步骤

10.3.2 外部社会化媒体网站审核步骤

10.4 小结

第11章 声誉管理：战略与协作

11.1 案例研究：Domino 担 声誉攻击

11.1.1 什么方面出了问题

11.1.2 他们做了什么正确的事

11.2 毁灭品牌资产的企图：从标志到品牌

11.3 主动管理你的声誉

11.3.1 联络帖子作者和域所有者

11.3.2 要求删除内容

11.3.3 诉诸法律手段

## <<社会化媒体与企业安全>>

- 11.3.4 利用搜索引擎优化
- 11.4 社会化媒体战略的禅意和艺术
  - 11.4.1 当市场活动出现问题的时候
  - 11.4.2 创建自己的社会化网络
- 11.5 危机的时候你找谁
- 11.6 用事故管理减小声誉风险
- 11.7 小结

### 第四部分 监控与报告

#### 第12章 人力资源：监控与报告

- 12.1 案例研究：Facebook帖子导致解雇
- 12.2 人力资源部进行的监控
  - 12.2.1 符合性
  - 12.2.2 监控的焦点
  - 12.2.3 HR可以禁止社会化媒体活动吗
- 12.3 如何监控员工的使用情况
- 12.4 如何使用社会化媒体监控可能聘任的员工
- 12.5 基线监控和报告需求
- 12.6 策略管理
- 12.7 小结

#### 第13章 资源利用：监控与报告

- 13.1 案例研究：该如何回应
- 13.2 谁、什么、何地、何时、如何
- 13.3 技术
  - 13.3.1 URL过滤
  - 13.3.2 数据搜索和分析
- 13.4 知识产权
- 13.5 版权
- 13.6 事故管理
- 13.7 报告的衡量标准
- 13.8 小结

#### 第14章 财务：监控与报告

- 14.1 案例研究：预算的难题
- 14.2 有限预算下的社会化媒体安全
  - 14.2.1 Google Alerts
  - 14.2.2 Google Trends
  - 14.2.3 Google Blog搜索
  - 14.2.4 Google Insights for Search
- 14.3 在大预算下的社会化媒体安全
  - 14.3.1 Radian
  - 14.3.2 Lithium (前Scout Labs)
  - 14.3.3 Reputation.com
- 14.4 培训成本
- 14.5 小结

#### 第15章 运营管理：监控与报告

- 15.1 案例研究：成功使用社会化媒体
- 15.2 确保遵循安全惯例所需的监控类型
- 15.3 数据丢失管理：工具与实践

## <<社会化媒体与企业安全>>

15.3.1 警告系统

15.3.2 使用趋势跟踪

15.3.3 日志文件存档

15.4 监控和管理工具

15.4.1 监控评论

15.4.2 监控员工

15.5 跟踪员工使用情况

15.5.1 跟踪员工使用情况的好处

15.5.2 策略更改的分发

15.5.3 跟踪社会化媒体新闻

15.6 小结

第16章 声誉管理：监控与报告

16.1 案例研究：不受控制的声誉破坏

16.2 在线声誉管理

16.2.1 牌资产

16.2.2 声誉管理和员工

16.3 建立一个监控系统

16.4 建立一个基线并与历史时期比较

16.5 如何更好地利用声誉信息

16.6 小结

第五部分 社会化媒体3.0

第17章 评估你的社会化媒体战略

17.1 JAG做得如何

17.2 前方的挑战

17.2.1 确定实施过程

17.2.2 安全是一个活动的目标

17.2.3 管理和策略的持续更改

17.2.4 检查你的来源

17.2.5 验证系统正在变化

17.2.6 品牌攻击难以跟踪

17.3 主动声誉管理

17.3.1 响应

17.3.2 报告

17.3.3 补救

17.4 小结

第18章 社会化媒体安全的未来

18.1 包罗万象的互联网

18.2 发展中的对“全球脑”的威胁

18.2.1 失控

18.2.2 产品和数据盗窃

18.2.3 隐私的侵蚀

18.2.4 以地理位置为目标

18.2.5 对家用设备的攻击

18.2.6 对品牌的攻击

18.2.7 “你是我的了！”

18.2.8 不一致的法规



## <<社会化媒体与企业安全>>

18.3 进攻是最好的防守

18.4 深入考虑安全模型

18.5 小结

附录 资源指南

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>