• 规划 • 实施 • 管理 •

Mc Graw Hill Education

安全计划与灾难恢复

Security Planning & *Disaster Recovery*

- 创建并成功实施企业安全计划和灾难恢复计划
- 识别当前系统中难以检测的安全隐患
- 学习合理的安全预算策略，部署有效的应急响应计划

〔美〕Eric Maiwald
William Sieglein 著
孙东红 刘 勇 段海新 译

人民邮电出版社
POSTS & TELECOM PRESS

安全计划与灾难恢复

[美] Eric Maiwald William Sieglein 著

孙东红 刘 勇 段海新 译

人民邮电出版社

图书在版编目（CIP）数据

安全计划与灾难恢复/（美）梅沃德（Maiwald, L.），（美）西格莱因（Sieglein, W.）著；孙东红，刘勇，段海新译. —北京：人民邮电出版社，2003.11
ISBN 7-115-11684-9

I. 安… II. ①梅… ②西… ③孙… ④刘… ⑤段… III. ①安全管理—计划②紧急事件—处理 IV. X93

中国版本图书馆 CIP 数据核字（2003）第 085204 号

版 权 声 明

安全计划与灾难恢复

◆ 著 [美] Eric Maiwald William Sieglein
译 孙东红 刘 勇 段海新
责任编辑 李 际

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www. ptpress.com.cn
读者热线 010-67132705
北京汉魂图文设计有限公司制作
北京鸿佳印刷厂印刷
新华书店总店北京发行所经销

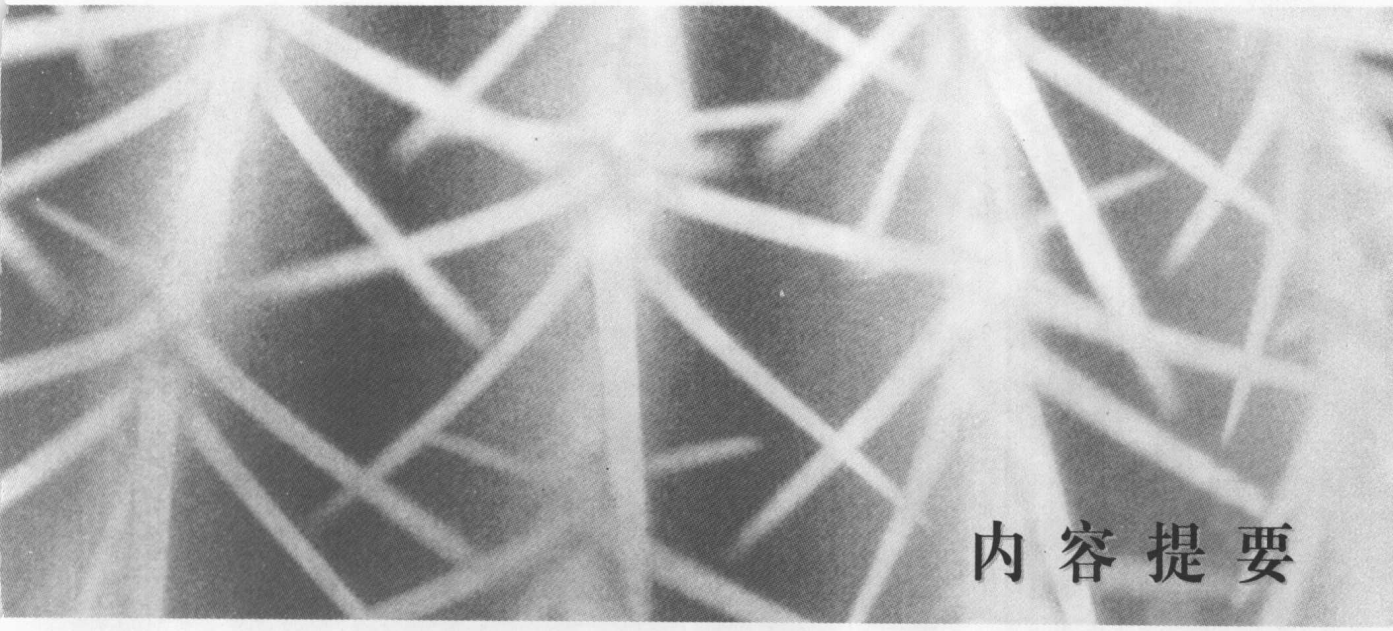
◆ 开本：787×1092 1/16
印张：15.25
字数：359 千字 2003 年 11 月第 1 版
印数：1-3 500 册 2003 年 11 月北京第 1 次印刷

著作权合同登记 图字：01－2002－4129 号

ISBN 7-115-11684-9/TP・3605

定价：32.00 元

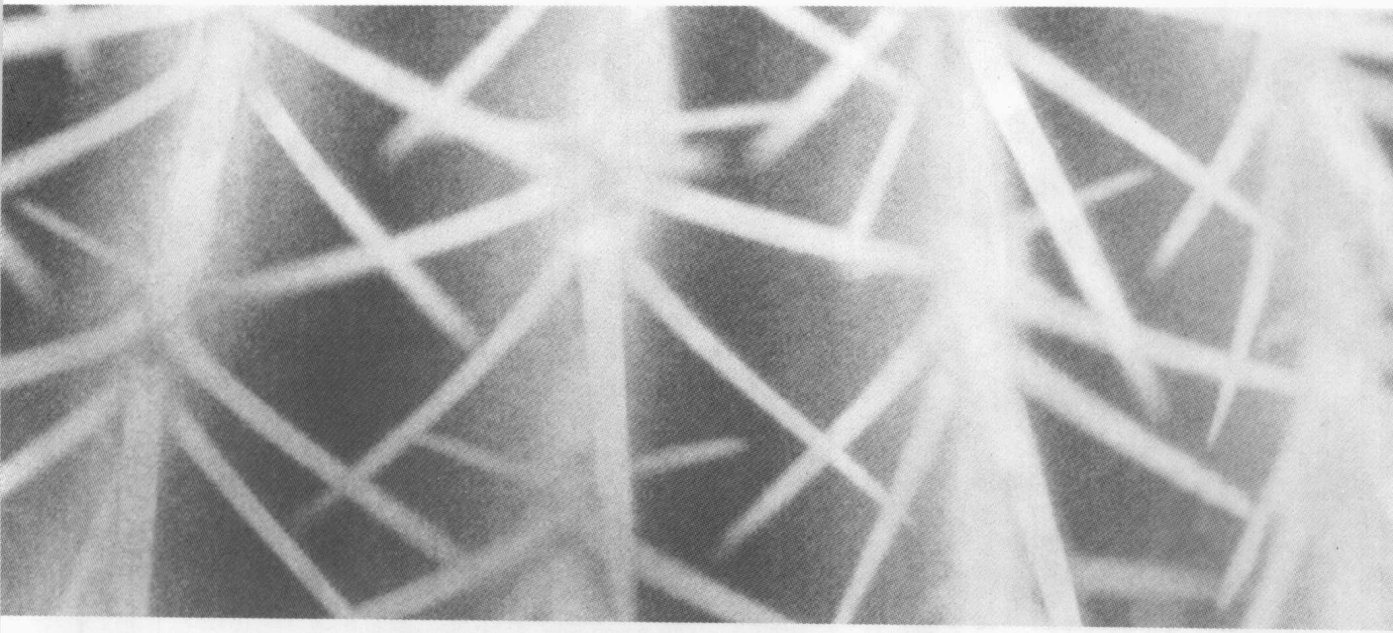
本书如有印装质量问题，请与本社联系 电话：(010)67129223



内容提要

要解决信息安全问题不是简单地依靠安全技术人员就可以的，对于所有从事IT业务或者倚仗IT基础设施来辅助业务运作的公司或组织而言，制定适合本单位的安全计划是非常重要的。本书层次清晰地介绍了安全计划的建立、实施和管理，紧急事件处理等方面的具体细节。针对安全计划所涉及的政策、过程、审计、监控、培训、时间和资金投入以及意外事件的应急处理等进行了专题讲解。本书内容环环相扣，具有很强的指导性和可实践性。

本书适合政府、企业等行业中IT相关部门的管理人员，以及网络和信息安全服务行业的从业人员使用。

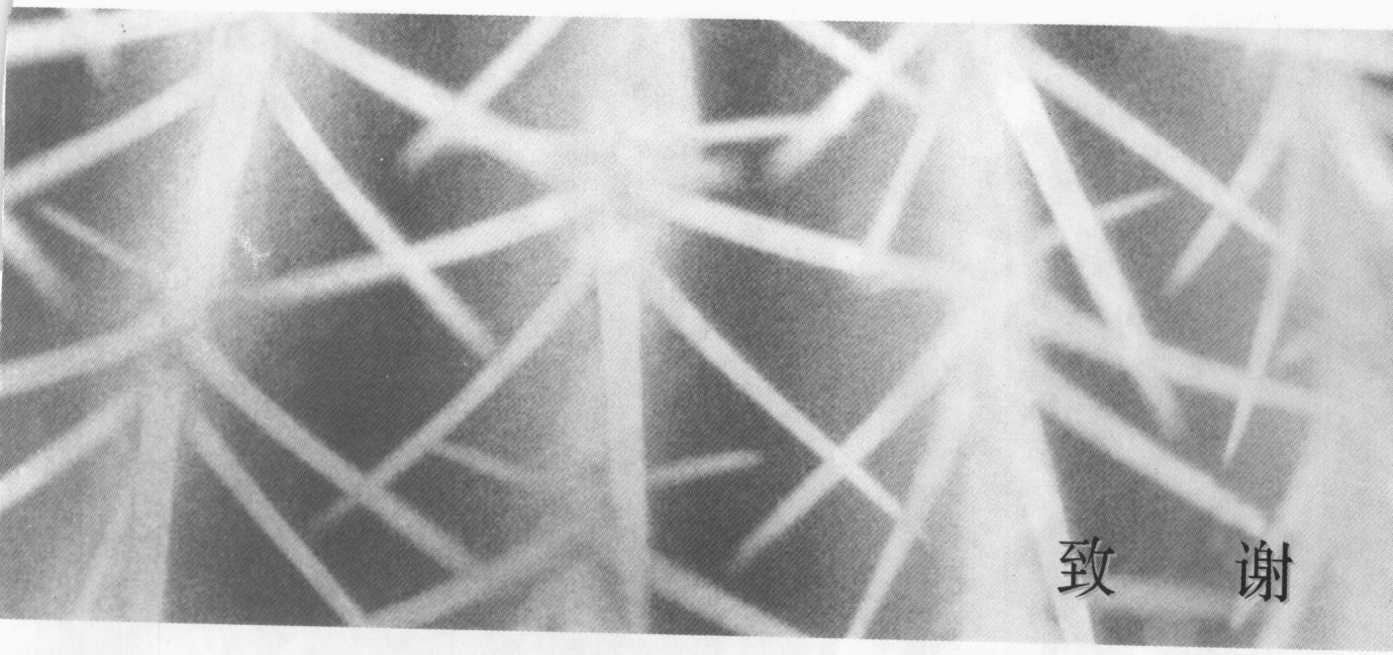


谨将此书献给我的妻子 Kay 以及两个儿子 Steffan 和 Joel，为了完成这本书，他们失去了很多可以和我一起快乐玩耍的时间，忍受了漫长的等待。感谢他们给予我的支持。

——EM

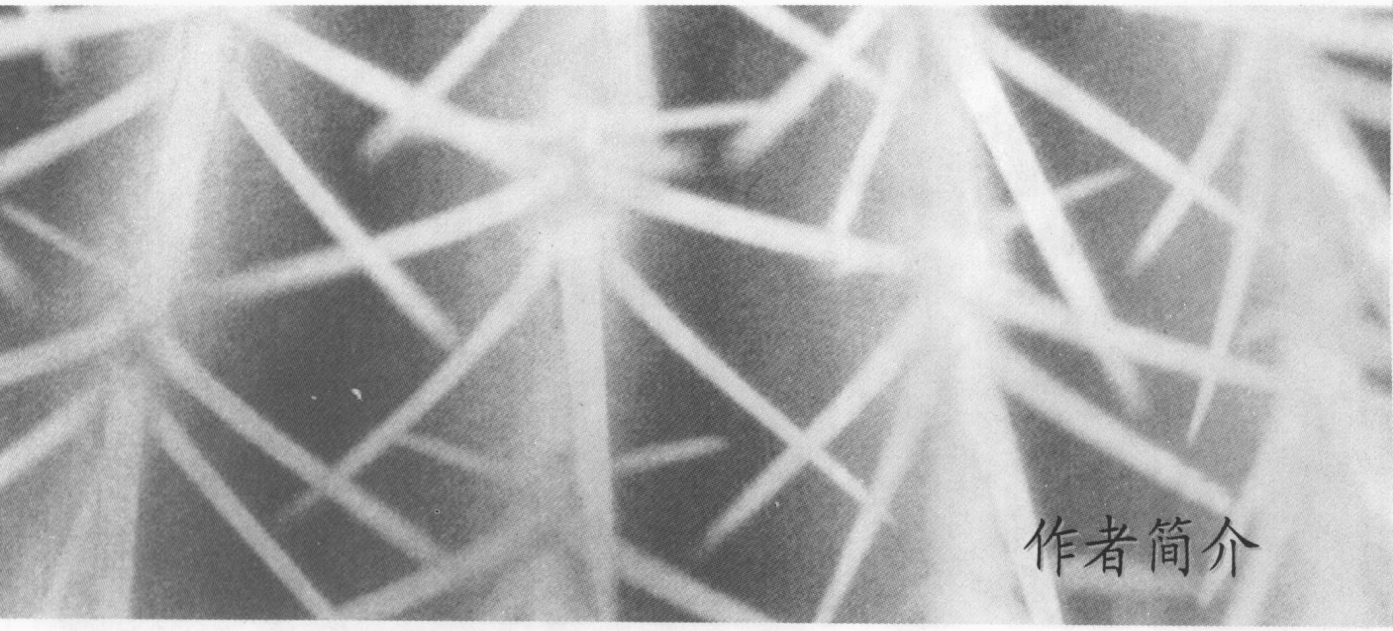
谨将此书献给我亲爱的妻子 Jane —— 她不是《奥赛罗》或《李尔王》中的 Jane，我（WS）也不是王室成员。奉献给我的孩子们 Kyle、Haley 和 Maggy —— 太棒了，我终于可以抽开身了！

——WS



致　谢

这本书是在很多朋友的帮助下才得以完成的。尤其是来自 Fortrex 公司的同事们，从事 HIPAA 规则工作的 Lee Kelly 和从事 GLBA 研究的 Andrew Waltz 的帮助，在此我向他们表示感谢。此外，我们还要感谢技术编辑 Ben Rothke 的大力支持，以及 McGraw-Hill/Osborne 的员工，特别是 Jane Brownlow、Emma Acker 和 Janet Walden，正是因为有了他们的帮助此书才能够顺利出版。



作者简介

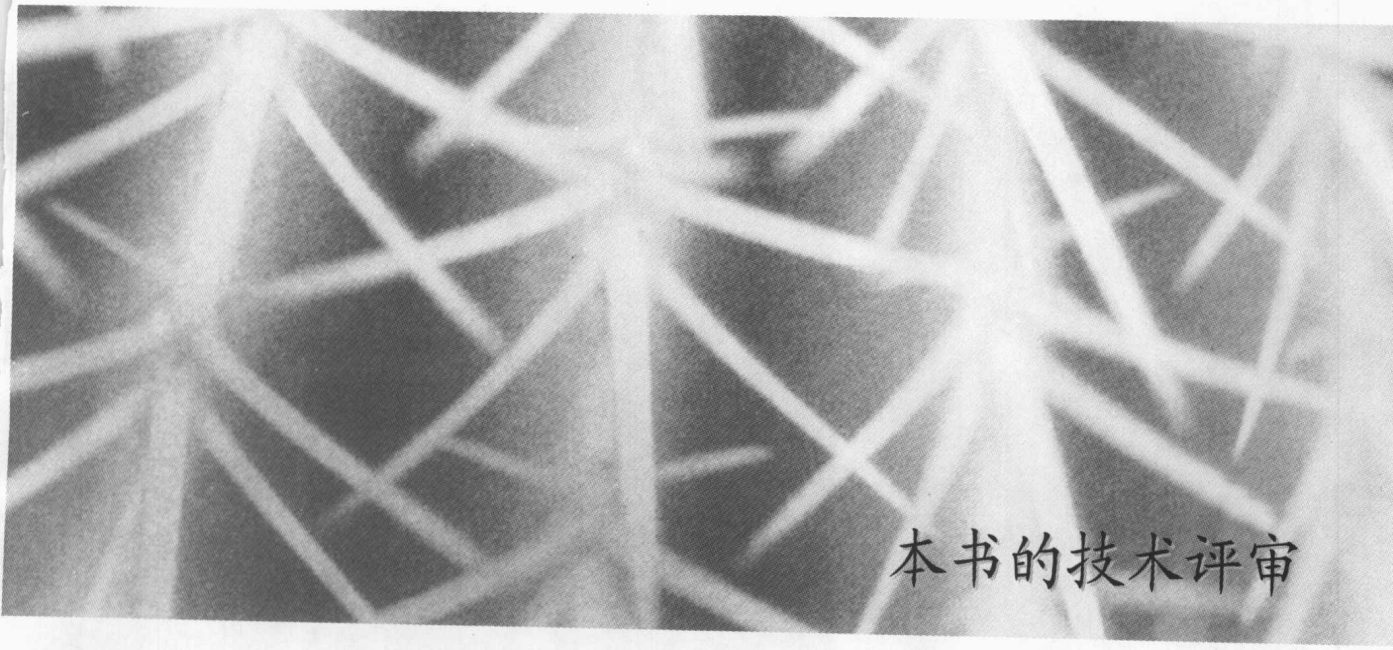
Eric Maiwald 是 Fortrex 公司的首席技术官，负责管理公司全部的安全研究和培训活动以及 Fortrex 网络安全中心的运行工作。此外，Maiwald 先生还参与过很多其他类型的工作，比如对大型的金融机构、服务公司和生产厂商进行风险评估，制定企业的开发策略和部署安全解决方案等等。作为咨询顾问、安全主管和开发者，他在安全领域有着丰富的工作经验。Maiwald 拥有 Rensselaer 理工学院的电子工程理学学士学位、Stevens 科技学院的电子工程学硕士学位，并且是认证的信息系统安全专家（CISSP）。

Maiwald 是以下专利的著名发明家，专利号分别为：5 577 209“Apparatus and Method for Providing Multi-level Security for Communications Among Computers and Terminals on a Network”；5 872 847 “Using Trusted Associations to Establish Trust in a Computer Network”；5 940 591“Apparatus and Method for Providing Network Security”；以及 6 212 636“Method for Establishing Trust in a Computer Network via Association”。

Maiwald 经常出席一些知名的安全性会议。他还编写了由 McGraw-Hill/Osborne 出版的 *Network Security: A Beginner's Guide*，并参与编写了同样是由 McGraw-Hill/Osborne 出版的 *Hacking Linux Exposed* 和 *Hacker's Challenge* 两本书。

William Sieglein 是 Fortrex 公司的安全服务经理，管理公司所有安全咨询和专业服务。Sieglein 还负责 Fortrex 管理客户信息的安全项目、风险评估、制定开发策略以及部署安全解决方案。他在 IT 领域拥有二十多年的工作经验，在信息安全方面尤为出色。Sieglein 曾获得了马里兰大学计算机科学理学学士学位和约翰霍普金斯大学工程管理理学硕士学位。

Sieglein 在各类出版物上发表过大量文章，其中包括 *Business Credit Magazine*、*Security Advisor* 和 *CMP's iPlanet*，同时他还曾经为这些出版社担任过几个月的安全顾问。Sieglein 一直是某些组织的特约发言人，其中有国际信息系统审计与管理协会（ISACA）、联合特种作战指挥部（JSOC），以及美国行业安全协会（ASIS）。

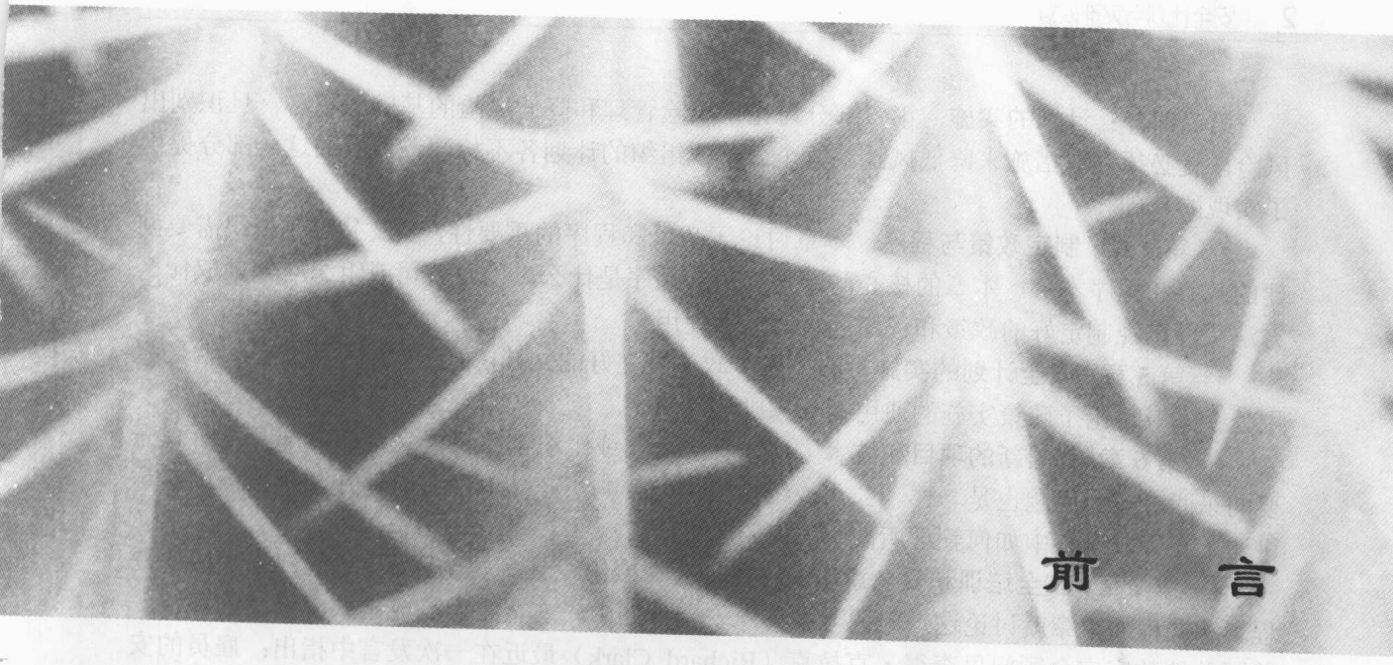


本书的技术评审

Ben Rothke 是 trustEra（www.trustEra.com） 的首席顾问。他的专业领域为 PKI、系统安全设计与实现、HIPAA、加密、安全体系结构与分析、防火墙配置和安全检查、密码技术以及安全政策开发等。Rothke 最初受雇于 Baltimore Technology、Ernst & Young 和 Citibank，曾为财富 500 强之中的很多公司提供过信息安全解决方案。

他经常在行业大会上发言，并且为许多计算机期刊撰稿。目前，他为 *Unix Review* 撰写专栏，还在 *Security Management* 杂志上对安全性书籍每月发表一次书评。

Rothke 是认证的信息系统安全专家（CISSP）、认证的机密主管（CCO），同时还是 ISSA、ICSA、IEEE、ASIS 和 CSI 的成员，目前在其纽约的办公室办公。



前　言

现在是以电子信息为中心的时代，各类公司或组织倚仗 IT 基础设施来辅助业务的运作，甚至有些公司或组织将其作为业务的核心。对这些公司或组织而言，安全、可靠的计算和通信是至关重要的。这些公司和组织，开始理解信息安全的重要性，他们纷纷在 CIO 的指导下制定安全计划。

除了人员和技术以外，信息安全计划还包括许多其他的内容，涉及政策、过程、审计、监控以及时间和资金上的投入。本书旨在向公司或组织提供安全计划的宽泛的概述：安全计划是什么？应该包括哪些人？必须要做什么事情？如何使之与整个公司或组织相适应？等等。

本书面向安全专家，他们必须解决公司或组织的安全管理方面的问题。在现在的经济条件下，许多公司或组织没有能力雇用人员专门从事安全工作。通常，负责这项任务的是没有经过专门的安全培训的 IT 专家。本书为这些人提供了指导性的路线图。

全书分为四个主要部分和内容丰富的附录。

第一部分：制定计划的指导原则　第一部分旨在针对安全计划的基本问题提供指导。在这一部分，我们概述了信息安全的任务、法律和法规、风险识别等基本概念。

- **第 1 章：信息安全计划的任务**　第 1 章讨论了信息安全计划的整体重要性，叙述了它在公司或组织中的位置，以及谁负责建立它的许可、任务、责任和权威。本章还进一步讨论了信息安全经理（及其部门）与公司或组织的其他人员、部门之间的关系。信息安全计划不可能凭空建立，也不能建立在恶劣的组织关系的基础之上。
- **第 2 章：法律和法规**　许多行业都必须遵守的法规。有些法规可能对安全计划产生影响。于是，安全部门对于法规要求的理解就变得十分重要。有些情况下，法律和法规明确规定必须实行信息安全计划。
- **第 3 章：评估**　本章旨在讲述公司或组织如何辨别自己的信息安全状况，包括各种类型的评估信息，以及何时应该进行评估，何时不应该进行评估。

第二部分：计划的实施 第二部分讨论了风险管理和降低风险的基础问题。一旦识别出风险，就必须采取措施来降低风险。每个公司或组织的计划各不相同，本书的这一部分提供了实现的基础。

- **第 4 章：制定政策与程序** 本章讨论了政策和程序的重要性，以及公司或组织需要创建的政策和程序本身。本章的核心问题是创建的顺序是什么，以及公司或组织应该采取什么方法买进已经制定好的政策和程序并将其投入使用。
- **第 5 章：安全计划的实施** 即便安全政策是完好的文档，但是如果不去实施，就毫无用处。本章讨论了政策实施的通用指导原则。
- **第 6 章：部署新的项目和技术** 任何一个公司或组织都不可能完全在内部开发所有需要的东西。安全问题也是一样。公司或组织很可能会购买产品，并在内部开发新项目。本章讲述了在开发过程中如何管理所面临的风险。
- **第 7 章：安全培训和安全意识** 为了使公司或组织具备安全意识，必须建立相应的课程表和课程，本章就讨论这一问题。在信息安全计划中，安全意识是成本效率最高的环节。美国总统数字安全顾问里查得·克拉克（Richard Clark）最近在一次发言中指出：雇员的安全意识对于公司或组织的安全计划来说至关重要。他还说到，在未来几个月内，他将和联邦政府一起向工业界强调这一问题。
- **第 8 章：安全监控** 安全计划到位以后，如何知道它是否正在发挥作用？惟一的办法是进行监控。本章叙述了用于监控的更多有用的方法。

第三部分：安全计划的管理 在公司或组织内部，安全计划和其他计划相比没有什么不同。一旦建立完成并正常运行，就必须进行恰当的管理和控制。这一部分就讨论这一问题。

- **第 9 章：安全预算** 每一个公司或组织都有预算过程。安全部门必须和其他部门一样通过这个过程。因此，很重要的一点就是安全部门把预算做好。
- **第 10 章：安全人员** 虽然不是每个安全计划都安排了安全人员，但是很多计划是这样做的。挑选合格的安全人员，改善他们的技能，保证安全计划得以实施。本章讨论了队伍的构成问题，以及如何寻找合适的人选。
- **第 11 章：报告** 最后是报告问题。没有报告，公司或组织就无法衡量安全部门的效率。几乎很少有安全 ROI（但是这正在改变），因此必须有其他的尺度用以衡量部门的业绩。

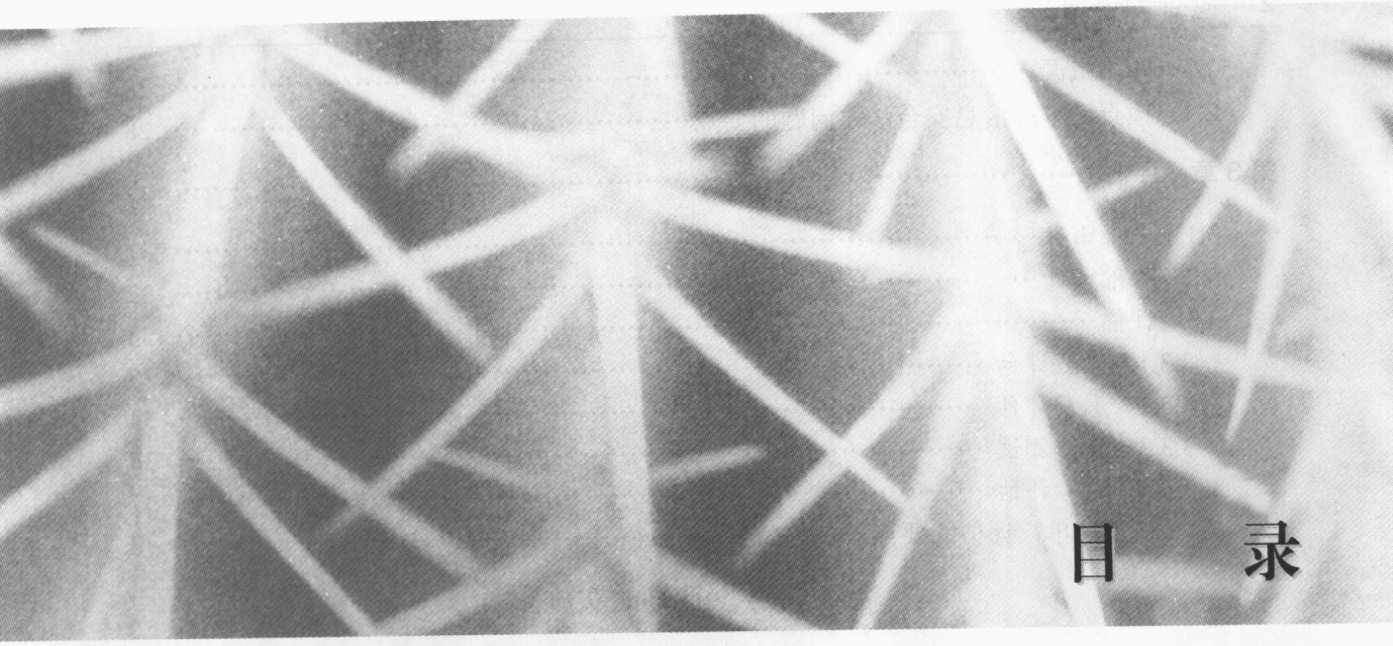
第四部分：应急事件响应 所有的计划、风险识别、风险缓解和管理任务都能够帮助公司或组织管理风险。然而，没有人能够完全消除风险。本书的这一部分将讨论如何处理突发的事件和灾难。

- **第 12 章：事件响应** 糟糕的事情发生了。安全计划竭力避免发生事件，但最终事件还是发生了。当出现意外事件时，安全部门必须随时准备好各种应对措施。
- **第 13 章：制定应急计划** 业务可能发生各种形式和规模的灾难。由于公司或组织对 IT 基础设施的依赖程度如此之高，以至于很有必要制定 IT 灾难恢复计划，并保持随时更新。该计划应当说明政策、程序、角色和责任，用以作好应对各种灾难的准备。本章解释了制定 IT DRP 的关键步骤。

- **第 14 章：灾难响应** 公司或组织对灾难的响应工作，与对灾难的准备工作是同等重要的。通常，由于出现了未曾预料的情况，对灾难的响应偏离了制定的计划。本章讨论如何对严重灾难做出恰当的响应。

第五部分：附录 第五部分的 3 个章节对全书起补充作用。这些章节旨在帮助读者回答有关安全和实施强大计划方面的一些特定问题。

- **附录 A：处理审计** 审计在现实生活中比比皆是。每个公司或组织都要通过审计，可能是内部审计，也可能是外部审计。安全团队必须是审计的一部分，是公司或组织的响应的一部分。
- **附录 B：安全外包** 最近，安全外包成为一个真实的话题。许多新的安全公司纷纷成立，他们销售某种安全服务。这可能会影响到公司或组织的安全，也可能是完成安全部门职能的一条高效的途径。
- **附录 C：管理新的安全项目** 附录 C 是第 6 章的延续，继续讨论构建新的安全项目，而不是新业务项目的安全问题。
- **附录 D：** 安全计划与灾难恢复蓝图。



目　录

第一部分　制定安全计划的指导原则

第 1 章　信息安全计划的任务 …… 3

1.1　正确的开端 …… 4
1.2　确定安全部门的任务 …… 5
1.2.1　报告的机构 …… 5
1.2.2　任务声明 …… 6
1.2.3　长期目标 …… 7
1.2.4　短期目标 …… 8
1.3　关系 …… 8
1.3.1　技术关系 …… 8
1.3.2　业务关系 …… 11
1.4　检查清单：计划的关键任务 …… 14

第 2 章　美国的相关法律和法规 …… 15

2.1　与执法部门合作 …… 17
2.2　法律背景 …… 17
2.2.1　计算机欺骗和滥用法（1986 年版） …… 18
2.2.2　电子通信隐私法（1986 年版） …… 19
2.2.3　计算机安全法（1987） …… 21
2.2.4　国家信息基础设施保护法（1996） …… 21
2.2.5　Gramm-Leach-Bliley 金融服务现代化法案（GLBA） …… 22
2.2.6　医疗保险信息携带及责任法案（HIPAA） …… 25

2.3 网络资源 …… 28
2.4 检查清单：信息安全法律问题的要点 …… 28

第 3 章 评估 …… 29

3.1 内部审计 …… 31
3.2 外部审计 …… 32
3.3 评估 …… 33
3.3.1 自我评估 …… 33
3.3.2 漏洞评估 …… 34
3.3.3 穿透测试 …… 35
3.3.4 风险评估 …… 37
3.4 检查清单：评估的要点 …… 40

第二部分 计划的实施

第 4 章 制定政策与程序 …… 43

4.1 政策的目的 …… 44
4.2 制定政策 …… 45
4.2.1 可接受使用政策（AUP） …… 45
4.2.2 信息安全政策 …… 46
4.3 现有文档的处理 …… 51
4.4 使他们认可 …… 52
4.5 政策审查 …… 53
4.6 检查清单：制定政策与程序的要点 …… 54

第 5 章 安全计划的实施 …… 55

5.1 从何处开始 …… 57
5.1.1 建立计划书 …… 57
5.1.2 风险评估 …… 59
5.1.3 降低风险的计划 …… 59
5.1.4 制定政策 …… 61
5.1.5 解决方案的部署 …… 61
5.1.6 培训 …… 61
5.1.7 审计和报告 …… 61
5.1.8 重新再做一遍 …… 62
5.2 和系统管理员们一起工作 …… 63
5.3 和管理者一起工作 …… 64
5.4 教育用户 …… 66
5.5 检查清单：安全计划实施的要点 …… 66

第 6 章 部署新项目和新技术 …… 67

6.1 新的业务项目 …… 68
6.1.1 需求定义 …… 69
6.1.2 系统设计 …… 71
6.1.3 内部开发 …… 81
6.1.4 第三方产品 …… 81
6.1.5 测试 …… 82
6.1.6 试运行 …… 82
6.1.7 完全产品化 …… 83
6.2 检查清单：部署业务项目的要点 …… 83

第 7 章 安全培训和安全意识 …… 85

7.1 用户意识 …… 86
7.2 管理者意识 …… 87
7.3 安全小组的培训和意识 …… 88
7.4 培训方法 …… 89
7.4.1 工作描述 …… 89
7.4.2 始业教育 …… 90
7.4.3 可接受使用政策(AUP) …… 90
7.4.4 正式的课堂培训 …… 90
7.4.5 研讨会和自助会议 …… 91
7.4.6 时事通讯和网站 …… 92
7.4.7 大型活动 …… 93
7.4.8 会议 …… 93
7.5 检查清单： 安全培训和安全意识的要点 …… 94

第 8 章 安全监控 …… 95

8.1 政策监控 …… 96
8.1.1 意识 …… 96
8.1.2 系统 …… 97
8.1.3 员工 …… 98
8.1.4 计算机的使用政策 …… 98
8.2 网络监控 …… 99
8.2.1 系统配置 …… 99
8.2.2 网络攻击 …… 99
8.2.3 网络监控机制 …… 100
8.3 审计日志的监控 …… 101
8.3.1 非授权的访问 …… 101
8.3.2 不合适的行为 …… 101

8.3.3 有效日志监控机制 …… 102
8.4 安全漏洞监控 …… 103
8.4.1 软件补丁 …… 103
8.4.2 配置问题 …… 103
8.4.3 识别安全漏洞的机制 …… 104
8.5 检查清单：安全监控的要点 …… 106

第三部分 安全计划的管理

第 9 章 安全预算 …… 109

9.1 确定需求 …… 110
9.2 制定预算 …… 111
9.3 其他事项 …… 112
9.3.1 人员需求 …… 112
9.3.2 培训费用 …… 113
9.3.3 软件和硬件维护 …… 114
9.3.4 外部服务 …… 115
9.3.5 新产品 …… 116
9.3.6 不可预料的费用 …… 117
9.4 严格执行预算 …… 117
9.5 检查清单：安全计划预算中的要点 …… 117

第 10 章 安全人员 …… 119

10.1 技能领域 …… 120
10.1.1 安全管理能力 …… 120
10.1.2 政策开发能力 …… 121
10.1.3 体系结构设计能力 …… 122
10.1.4 研究能力 …… 122
10.1.5 评估能力 …… 122
10.1.6 审计能力 …… 122
10.2 雇用好的员工 …… 123
10.2.1 职业道德 …… 123
10.2.2 能力与经验 …… 123
10.2.3 个性品质 …… 124
10.2.4 认证证书 …… 125
10.3 小型机构 …… 126
10.3.1 职员的技能 …… 126
10.3.2 寻找外部的技能 …… 127
10.4 大型机构 …… 128

10.4.1 安全部门的基本编制 …… 128
10.4.2 寻找外部的技能 …… 128
10.5 检查清单：雇用职员的要点 …… 129

第 11 章 报告 …… 131

11.1 项目计划的进度 …… 132
11.2 安全的状态 …… 133
11.2.1 测度 …… 133
11.2.2 风险的测量 …… 135
11.3 投资回报 …… 139
11.3.1 业务项目 …… 140
11.3.2 直接的回报 …… 140
11.4 意外事件 …… 140
11.4.1 事件的事实描述 …… 140
11.4.2 被利用的安全漏洞 …… 141
11.4.3 采取的行动 …… 141
11.4.4 建议 …… 141
11.5 审计 …… 141
11.6 检查清单：安全报告中的要点 …… 142

第四部分 如何响应意外事件

第 12 章 事件响应 …… 145

12.1 事件响应组 …… 146
12.1.1 小组成员 …… 146
12.1.2 领导 …… 148
12.1.3 授权 …… 148
12.1.4 小组筹备 …… 148
12.2 事件确认 …… 149
12.2.1 事件是什么 …… 149
12.2.2 要查找什么 …… 149
12.2.3 服务台的帮助 …… 151
12.3 升级 …… 151
12.3.1 调查 …… 152
12.3.2 收集证据 …… 152
12.3.3 决定如何响应 …… 153
12.4 控制措施 …… 153
12.5 事件根除 …… 154
12.6 文档 …… 155

12.6.1 事件发生前的文档 …… 155
12.6.2 事件处理过程中的文档 …… 156
12.6.3 事件处理后的文档 …… 157
12.7 法律问题 …… 157
12.7.1 监控 …… 157
12.7.2 证据收集 …… 158
12.8 检查清单：事件响应的要点 …… 158

第 13 章 制定意外事件的应急计划 …… 159

13.1 灾难定义 …… 161
13.2 确定重要的系统和数据 …… 162
13.2.1 业务影响分析 …… 162
13.2.2 采访过程 …… 164
13.3 准备 …… 164
13.3.1 风险分析项目 …… 164
13.3.2 资产清单 …… 165
13.3.3 获得资金 …… 166
13.3.4 支出的理由 …… 167
13.3.5 资金分配 …… 167
13.3.6 组织间的合作和合作政策 …… 167
13.4 把 DPR 工作组和指导委员会一起考虑 …… 168
13.5 常规程序 …… 169
13.6 资源 …… 171
13.7 检查清单：应急计划的要点 …… 172

第 14 章 灾难响应 …… 173

14.1 真实性检查 …… 174
14.1.1 先发生的事情先处理 …… 174
14.1.2 损失评估 …… 174
14.2 定义权威和工作组 …… 175
14.2.1 工作组的召集 …… 176
14.2.2 可用技术评估 …… 177
14.2.3 设定优先次序 …… 177
14.2.4 设定目标 …… 177
14.3 是否遵守计划 …… 178
14.4 灾难的阶段 …… 178
14.4.1 灾难响应阶段 …… 179
14.4.2 恢复运作阶段 …… 180
14.4.3 恢复生产阶段 …… 181