WILEY

HZ BOOKS

IT安全面试攻略

IT Security Interviews Exposed:

Secrets to
Landing Your Next
Information Security Job

(美) Chris Butler; Russ Rogers; Mason Ferratt; Greg Miles; Ed Fuller; Chris Hurley; Rob Cameron; Brian Kirouac 著

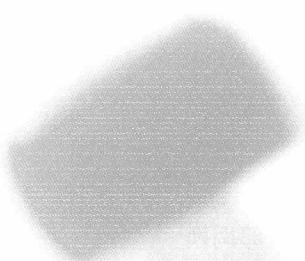
李波 卢敏 费玮 等译

机械工业出版社
China Machine Press

IT安全面试攻略

IT Security Interviews Exposed:

Secrets to
Landing Your Next
Information Security Job



机械工业出版社
China Machine Press

Chris Butler，Russ Rogers，Mason Ferratt，Greg Miles，Ed Fuller，Chris Hurley

Rob Cameron，Brian Kirouac：IT Security Interviews Exposed: Secrets to Landing Your Next Information Security Job（ISBN:978-0-471-77987-2）

Authorized translation from the English language edition published by John Wiley & Sons, Inc.

图书在版编目（CIP）数据

IT安全面试攻略/（美）巴特勒（Butler, C.）等著；李波等译. —北京：机械工业出版社，2008.12

书名原文：IT Security Interviews Exposed: Secrets to Landing Your Next Information Security Job

ISBN 978-7-111-25507-9

Ⅰ. I…　Ⅱ. ①巴…　②李…　Ⅲ. 信息系统－安全技术　Ⅳ. TP309

中国版本图书馆CIP数据核字（2008）第171817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：盛东亮

北京牛山世兴印刷厂印刷 · 新华书店北京发行所发行

2009年1月第1版第1次印刷

186mm × 240mm · 10.5印张

标准书号：ISBN 978-7-111-25507-9

定价：29.00元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

本社购书热线（010）68326294

译 者 序

随着互联网的快速发展和国家信息化建设的稳步推进，信息安全受到了社会各界的普遍重视。据专业的人才资源网站统计，近年来人才市场对网络安全工程师的需求量骤增。分析人士认为，无论是就业前景、受重视程度、提升空间还是薪酬基数、薪酬增长预期等，信息安全职位较其他IT职位都更优越。

本书适合那些寻求信息安全职位的读者。尤其是第1章，它告诉读者怎样获取一份自己最满意的工作。这一章的立足点与普通技术人员的思考方式不大相同，融合了作者一些经过提炼的生活经验，这些都是值得我们认真学习的。

本书并不是一本讲解信息安全的技术书籍，如作者在前言中所述，本书仅仅是信息安全领域的简短指南，读者并不能依靠本书获取信息安全领域的某一具体方向上的深层次的技术细节。

书中各章都给出了面试时常见的问题和答案，这可以让读者在面试时成竹在胸，更有自信和把握。在安全技术的各章节，作者不但讨论了技术，还列举了主流厂商，对比了常见产品；不但讨论了技术的原理，还说明了技术间的优劣和发展历程。这让读者可以知其然，更知其所以然。

本书的翻译工作由卢敏组织，主要由李波、卢敏、费玮负责翻译，参加翻译的还有王志淋、高鹏飞、韩平、董启雄、汪顶武、张旭、安志琦、申明冉等。

由于时间仓促，译者的水平有限，尽管我们尽了自己最大努力，书中仍会有错误或不妥之处，希望读者不吝指正！您可以发送邮件到：libotudou@sohu.com。对您的批评和指正，我们表示真诚的感谢！

很高兴把这本书的中文版带给大家，祝您学习愉快、求职顺利！

2008年9月

作者简介

Chris Butler（CISSP, JNCIS-FWV, JNCIA-SSL, CCSE, IAM/IEM）是Intellitactics解决方案方面的资深工程师。Chris在网络和网络安全领域有丰富的经验。他是美国海军的退伍军人，服役期间的主要研究领域是密码学。Chris曾为多家保险公司、投资公司、软件公司、服务供应商和制药公司设计、实施和维护过大型网络。他还为很多美国政府机构提供过网络和安全方面的咨询服务，这些机构包括国务院、国防部和能源部。在他的职业生涯里，他还曾与那些主要的安全及网络厂商广泛地合作。他同样精通商业的和开源的网络和安全管理软件的开发。Chris曾用OPEN软件为很多大公司做过深入的应用分析，并为其设计网络模型。他还是IEEE计算机协会和SANS的成员。

Russ Rogers（CISSP, IAM/IEM）是一名高级网络安全分析师，Security Horizon公司的前任CEO、创始人之一。Russ是美国空军的退伍军人，曾在军队服役，并曾为国家安全机构、国防信息系统机构和其他联邦机构提供技术支持。他还是《The Security Journal》的主编。此外，他还是亚利桑那州先进技术大学（University of Advancing Technology）的网络安全教授。Russ是十多本信息安全书籍的作者、合著者或技术编辑，他在全世界范围内讲演并向听众提供安全方面的培训。他还是信息安全研究网站（www.securitytribe.com）中安全部落的创始人之一。他从马里兰大学（University of Maryland）获得了计算机科学专业的学士和硕士学位。

Mason Ferratt（JNCIS-FWV, JNCIA-M MSEE, BSME）是南卡罗莱纳州查尔斯顿的Juniper Networks公司的联邦系统工程师。他曾为很多政府部门实施过大型网络安全工程。他最近一个项目的合作对象就是国防部医学委员会，他的团队负责所有海军和陆军医院及诊所的网络安全。他的专长是入侵检测/防护、VPN加密、防火墙、内容过滤和远程访问设备保护。他曾做过网络工程设计、建模和为国务院做系统测试，以及为很多网络供应商（如Corvis Corporation、Corrigent Systems、Lucent Technologies、Ascend Communications和Network Equipment Technologies）做网络工程的售前和售后服务。他从乔治华盛顿大学（George Washington University）获得了电子工程学学士学位，从维吉尼亚大学（University of Virginia）获得了机械工程学硕士学位。他拥有Top Secret/SCI证书，是IEEE成员。

Greg Miles（CISSP, CISM, IAM/IEM）是Security Horizon公司的创始人之一、主席、首席财务官、首席安全顾问，是科罗拉多州专业的安全服务与培训顾问。他是美国空军退伍军人，曾在军队服役，负责为国家安全局、国防信息系统机构、空军空中指挥部和NASA提供全球的安全保证。Greg策划并管理了计算机事件响应小组（Computer Incident Response Teams, CIRTs）、计算机取证技术研发和信息安全培训。Greg曾在多家杂志和期刊上发表过文章，其中包括《The Security Journal》和与网络犯罪相关的《The International Journal》。他与参与编著了《Network Security Evaluation: Using the NSA IEM》（Syngress出版，ISBN：978-1597490351）和《Security Assessment: Case Studies for Implementing the NSA IAM》

（Syngress出版，ISBN：978-1932266962）。Greg是先进技术大学的网络安全讲师和科罗拉多州技术大学（Colorado Technical University，CTU）的指导老师。

Ed Fuller（CISSP, IAM/IEM）是Security Horizon公司的高级副总裁、首席运营官和首席安全顾问。他有着超过28年的操作、通信、计算机信息系统以及安全方面的经验。他是信息安全评估和Security Horizon培训的主要负责人。Ed曾担任了长达9年的信息安全评估小组负责人。他还曾做过其他公司的信息安全培训经理和高级安全顾问。Ed完整地参与了国防信息系统机构（Defense Information Systems Agency，DISA）的全球安全计划的建立、实施和维护，这直接支持领域安全业务（Field Security Operations，FSO）。他参与了系统安全工程性能完备模型（Systems Security Engineering Capability Maturity Model，SSE-CMM）的建立，并且是发展和维护信息保证性能完备模型（Information Assurance Capability Maturity Model，IA-CMM）的关键人物。Ed同时还是国家安全局（National Security Agency，NSA）信息安全评估方法学（INFOSEC Assessment Methodology，IAM）和信息安全评价方法学（INFOSEC Evaluation Methodology，IEM）的讲师。Ed在美国海军服役了23年后退休。Ed与他人一起编著了《Security Assessment: Case Studies for Implementing the NSA IAM》（Syngress出版，ISBN：978-1932266962）和《Network Security Evaluation: Using the NSA IEM》（Syngress出版，ISBN：978-1597490351）。同时，他经常在《The Security Journal》上投稿。

Chris Hurley（IAM/IEM）是一名资深的渗透测试员，在华盛顿特区工作。他是世界上“攻击驾驶”（WarDrive）的发明者，截至去年，都是他在负责组织DEF CON驾驶攻击竞赛。他独立编著或与他人合著了多部关于无线安全和渗透测试的书籍，其中包括《WarDriving & Wireless Penetration Testing》（Syngress出版，ISBN：978-1597491112）、《The Penetration Tester's Open Source Toolkit》（Syngress出版，ISBN：978-1597490214）、《InfoSec Career Hacking》（Syngress出版，ISBN：978-1597490115）和《Stealing the Network: How to Own an Identity》（Syngress出版，ISBN：978-1597490061）。

Rob Cameron（JNCIS-FWV, JNCIA-M, CCSP, CCSE+）是Juniper Networks公司的一名安全方案工程师。他最近为Juniper Networks设计的安全解决方案，被认为是最佳设计方案。Rob主要研究网络安全体系结构、防火墙部署、风险管理和高性能设计。他有着丰富的工作经验，6年间，他为超过325名顾客提供了咨询服务。他的主要著作有《Configuring Netscreen and SSG Juniper Firewalls》（Syngress出版，ISBN：978-1597491181）和《Configuring NetScreen Firewalls》（Syngress出版，ISBN：978-1932266399）。

Brian Kirouac（CISSP, IAM/IEM）是Security Horizon公司的技术总监和首席安全顾问。Brain有长达15年的IT从业经验。在进入Security Horizon公司之前，他曾在美国国内和国际的多家企业从事信息安全工作。他曾是一所大学的网络管理员，后来成为一名系统管理员，主攻UNIX和Windows操作系统。他还是一个地方性团体的主要技术安全专家。除了在Security Horizon公司供职，他还是国家安全局（National Security Agency，NSA）信息安全评估方法学（INFOSEC Assessment Methodology，IAM）和信息安全评价方法学（INFOSEC Evaluation Methodology，IEM）的讲师，以及NSA IA-CMM评估小组的成员。Brain还是《The Security Journal》的主要撰稿人，SANS的特约嘉宾和仲裁人，NASA绳系卫星会议的评审专家。

前　言

我意识到几乎所有人都会跳过这部分，直接进入内容目录部分。我对此深表遗憾。如果你恰巧看到前言这部分内容，希望能看完以下几句：本书总结概括了面试求职中需要了解掌握的有关信息安全领域的知识。我们所讨论的主题是安全专业人员最为关心的。不管怎样，我要邀请你更深入地阅读，因为下面都是重要的信息。

内容简介

本书是一个有关信息安全的简短指南。它短小精悍，但却能切中要害，恰到好处地讲解信息安全面试中需要了解掌握的知识。可以一页一页地精读这本书，也可以把它作为参考。不管你采用何种方式使用，总能从中学到东西。本书涉及的主题很广，从政策到薪水，从哈希函数到驾驶攻击最好用的芯片。本书的每一章都需要参阅相关的专业书籍才能很好地体现其价值，因此，我们尽可能地提供了相关资源。此外，我们特地使用URL的简易形式给出搜索条件，或是给出准确的搜索字串。例如：

Google “Security Exposed site:wiley.com.”

点击你看到的第一个链接，加入收藏，然后查看它。这真是非常简单。

适用对象

任何需要寻求有关信息安全职位的人都可以阅读本书。如果书中没有讨论某个特定的主题，我们会提供其他相关资源为你使用，以提高你的水平。

未提及内容

如果想要从本书中找到关于认证的内容，那么请你停下来，本书中并没有这些内容。你需要查看Microsoft、Novell和Cisco提供的相关认证资料，你会发现信息安全领域已经完全超出了这些认证资料所涵盖的内容。因此，我们选择不在书中讨论认证问题。说了这些，你还是想要你的答案，这里我给你一个答案：

“本书只涵盖这些内容，看与不看是你的自由！”

我所能说的就是，做好自己的功课。使用给出的工具来决定什么职位最适合你和接近你的兴趣。对待工作，我们每个人都有自己的想法和期望。如果你是为了赚钱，使用薪水测算来决定什么职位才适合你（参考第1章）。如果你在寻找跳槽机会，则可以使用网站中的工作板块，键入一些缩写词，看看现在有哪些认证比较吃香。

我的朋友Jim Feely建议我们讨论VoIP安全，因为有很多已经显露的威胁。Jim是对的，我们应该采纳他的建议。然而，我们并没有在本书中讨论该部分内容。或许我们可以在另外一本

书中讨论VoIP安全。如果你需要了解此类知识，请查阅如下参考资料：

- Google“NIST 800-58.”；
- Google“VoIP Security.”；
- 在站点www.voipsa.org中查找“VoIP Security Alliance”。

祝你在求职中好运！

致谢

此书的面世，是Eric Greenberg努力的结果，是他把我推荐给了Wiley。谢谢，Eric，真的非常感激！

感谢Carol Long接受了Eric的建议，让我来写这本书。她断定这样的一本书将会对求职者很有帮助，我完全赞同她的看法。

非常感谢Russ Rogers给我灌输了NSA IAM/IEM方法论思想，但我更感激的是，他能在这么短的时间内召集一帮各种研究领域的专家，参与到本书的编写中来。Russ也是本项目的技术编辑。他为保证每位成员努力工作做出了巨大贡献。非常感谢！

感谢Rob Cameron和Brian Kirouac，他们在我最需要的时候帮助了我。在编写该书期间，我经历了工作变动，如果没有他们，这本书（我负责的部分）就不会顺利完成。Rob帮助编写了防火墙技术一章，Brian则负责工具这一章。感谢，伙计们！

还要感谢我的挚友Mason Ferratt。我通过Mason了解了他的专业方向IDP/IPS，由此完成了该部分的编写。网络技术基础一章的编写过程就像是在猜硬币，Mason赢了。谢谢，Mason！

感谢Ed Fuller完成了安全技术基础一章。Ed有着多年的评估企业安全状况的经验，所以这一章完全由他负责。谢谢，Ed！

感谢Greg Miles完成了法律、政策和指南这一章。感谢Greg！

感谢Chris Hurley编写完成了无线网络这一章。Chris已经写过多本关于无线技术的书籍，所以他很出色地完成了任务。谢谢，Chris！

感谢Tom Dinse，他从头到尾浏览了整本书，并为每一章给出了注释。与他合作非常轻松，我期待与他的再次合作。

还要感谢我的好朋友Jim Feely，他对书中的每一章都提出了独特的见解。他为我修改本书提供了无数建议，使得这本书看起来更加通俗易懂。

感谢我的朋友Mara Cummings，他为第1章提供了很多深刻的建议。

感谢拷贝编辑Susan Christophersen和本书的发行人Joe Wikert。

最重要的一点，我要感谢我的妻子Tabatha，从始至终，她都很有耐心。我还要感谢我的孩子们，Ariel、Erie、Eliea、Adrie和Emerie，他们拥有不可思议的魔力，让我在写作过程中一直斗志昂扬。将来我一定会报答他们的。

致谢名单

执行主编

Carol Long

开发编辑
Tom Dinse
技术编辑
Russ Rogers
拷贝编辑
Susan Christophersen
编辑经理
Mary Beth Wakefield
产品经理
Tim Tate
副总裁和执委会出版人
Richard Swadley
副总裁和出版人
Joseph B. Wikert
排版
Kate Kaminski, Happenstance Type-O-Rama
校对
Kathryn Duggan
索引编制
Melanie Belkin
周年Logo设计
Richard Pacifico

目　录

第1章　寻找、面试、得到工作

如果你的目标是获取一份信息安全领域的工作，那么你是否拥有它所要求的技能呢？你是否知道自己想从这份工作中得到什么呢？你如何找到最适合你并且最符合你的职业规划的工作呢？在本书的后面章节中，我们将讨论与IT安全相关的话题，但是在这一章，我们只讨论你对工作的期望以及如何找到工作。

找到潜在雇主的要求和个人能力之间的最佳平衡点，稍微有些挑战性。我们将会介绍几种不同的求职方法，还会告诉你如何在你所拥有的信息的基础上，比较薪金，从而做出最好的选择。如果你实力超群，比较幸运，能够同时收到多份聘书，我们将讨论，在比较这些聘书的同时，怎样评价和权衡所有的工资条款。

1.1　资格

相当一部分雇主认为，应聘者理想的资格是拥有一个计算机科学专业或计算机工程专业的学位，还有更多的雇主会考虑将工作经历作为学位的补充。几年前，很难找到一个提供了恰当的信息安全和保障课程、足以使学生获取相关学位的学校。结果，具有不同理论背景、不同兴趣、不同技术能力的人，在信息安全领域却成了强有力的竞争者。以我12年来的经历而言，很惊讶地发现，主修英语的人成了网络安全工程师，主修商务的人进入了技术制造业，并充分展示了他们在分析性思维和解决问题的技能方面的杰出才能。

如上所说，你决不会看到IT安全职业的公开招聘会要求应聘者拥有艺术、历史或英语专业学位。拥有这些学位的人能胜任这个工作么？绝对可以！仅仅因为没有获得公认的计算机科学或计算机工程学士学位，为数众多的、能力出众的安全领域从业人员被忽视了。雇主们已经开始明白这一切，他们考虑用其他的方式来考评雇员的才智和分析思考能力，你可能被要求做一系列的性格或（和）能力测试。如果你正在申请一个对信息安全素质要求较高的政府部门职位，你很可能会进行这些测试。

要在IT安全领域取得成功，你必须拥有一颗聪慧的大脑，保持积极向上，并具有学习新技术的能力，最重要的是，一种与众不同的思维方式。本书将向你介绍这些你并不熟悉的思维方式，它们既巧妙也大巧若拙。比如，那些优秀的计算机科学与计算机工程专业的毕业生并不知道什么叫：最小特权、默认拒绝/许可和纵深防御，这些核心概念并没有包含在传统的计算机科学或计算机工程专业课程中，那些博学的从业者都是通过在工作或培训中来学习和理解它们的。

1.2　获得学位

不论是否已经取得了学位，只要你明确IT安全将是你的从业方向，那么，你就应该参加由美国国家安全局（National Security Agency，NSA）建立的国家资讯安全教育卓越中心

(Centers of Academic Excellence in Information Assurance Education，CAEIAE）的考试。据最近一次统计，在美国3500多个高级教育机构中，仅仅75个开始了通过国家安全局评估批准的信息安全课程。更多的消息，可以通过google搜索“CAEIAE”获取。

如果你想获得一份美国联邦政府的工作，那么获得地区性认证的学院或大学的学位基本上是必需条件。美国国家教育委员会只授权了6个地区性认证机构。无论你是否在寻找一份联邦政府的工作，对你而言，获得这么一个学位，绝对是一笔划算的投资。在google中搜索“Regional Accreditation”，确保你的学校得到其中某个地区性认证机构的授权。这6个地区性认证机构如下：

- 新英格兰学院与学校协会(NEASC)
- 美国北方中央学院与学校协会(NCA)
- 美国中部各州学院与学校协会(MSA)
- 美国南方学院与学校协会(SACS)
- 美国西方学院与学校协会(WASC)
- 美国西北方学院与学校协会(NWCCU)

如果你的学校并没有获取相应区域的代理授权，你就应该考虑转到一所有授权的学校。你必须知道，虽然不是全部，但几乎是所有的被地区性认证机构授权的学校只承认其他拥有授权的学校的学分，这也是你应该远离那些没有获得授权的学校的一个原因。

1.3 完美的工作

最好的工作是什么？你认真地想过你究竟想追求什么吗？希望你考虑的不仅仅是薪水。在本章后面，我们会深入地讨论一些比较工作机会的方法，以便你能做出最佳决策。

就像所有成功实施的IT方案一样，你也应该从需求分析开始，把寻找下一份工作看成一个小规模的高优先级项目。在寻找工作的过程中，采用系统的分析方法会让你事半功倍。

用一张纸或者你最擅长的电子数据表程序来开始你的分析。你首先必须忽略薪水这个因素，虽然这样做很困难。让我们先说说那些无形的收益，虽然定量分析它们可能比较难，但是它们却会严重影响你在工作中的健康状况和愉快感。

1.3.1 无形收益

下面这些收益可以定性分析，它们能够更好地平衡你的工作和生活，并使你对工作充满憧憬。找到尽可能多的这类收益，在评估它们的重要性的时候，确保你考虑了以下几点。

如果你已经结婚或者是一个单身父亲（母亲），你和那些单身青年对理想收益的需求绝对不一样。即使你现在还是单身，你对该问题的认识可能也会随着你在公司中的发展而改变。

1）员工至上：在过去的12年中，我们发现仅有一个公司宣称它的核心价值观是保障员工的幸福安康，大多数公司只关心产品、服务和利益。如果雇主懂得员工越快乐，其工作越有成效，我们也许能有更多具有吸引力的地方可以工作。在你面试时，记住询问人事经理，公司对员工承担了哪些义务。

2）以雇员为中心：很多公司因其创造的以雇员为中心的工作环境而出名。从Google中搜

索 “Top Tech 50”，可以获取科技公司的排名情况，看看你所申请的公司的排名是否靠前。在《Working Mother》杂志中排名前100的公司，也是寻找工作的理想地点，你可以通过www.workingmother.com查看详细情况。《福布斯》和《财富》杂志也提供这类公司排行榜。

3）工作－生活平衡：很多公司在工作-生活平衡这个哲学论题上不断取得进步。一些以前习惯于打着提高生产效率的幌子强迫员工加班的公司，逐渐放弃了他们的这一做法，转而鼓励员工养成更平衡的工作习惯。最终结果呢？在和谐的工作环境下，产生了更强的生产力和更高的员工忠诚度。

4）额外的休息时间：公司怎么为加班时间计酬？你是否因为新的计划，而不得不工作到深夜，甚至连周末都得不到休息？经常这样吗？大部分大公司为了执行技术更新，经常加班到深夜，或在周末加班，或者兼而有之。你现在申请的职位，也许并不会以小时计酬，不过，很多公司通过向员工提供额外的休息时间，以补偿其在晚上和周末的加班。你应该搞清楚，老板是否会对员工的加班提供补偿，公司可能通过提供额外的休息时间或者加班工资来补偿。当然如果你足够幸运，也可能鱼与熊掌兼得。

5）远程办公：基于以下的理由，远程办公可能是一个公司所能提供的最大收益。

- 它可以减少员工日常往返上下班的压力；
- 它可以减少你的保险费用，以及你的汽车的自然磨损；
- 它将极大地减少你的油费；
- 员工工作时精力将更集中，通常也会更快乐。

远程办公每年可以节约数千美元的开支，然而，一些雇主仍然处于适应这些变化的过程中（他们还停留在20世纪80年代）。不幸的是，相当多的从20世纪拼杀出来的雇主觉得，如果你不在他们面前工作的话，他们就不能真正地管理你。幸好还有很多公司对远程办公持支持态度，无论如何，对雇主和雇员而言，这是一个双赢的局面。在你能呆在家里完成同样工作的情况下，公司将不用再为办公室的每平方英尺支付数百美元的租金。过去数年中，联邦政府、州政府、地方政府都认识到远程办公的好处，比如减少道路磨损、缓和交通阻塞等。为了鼓励允许远程办公的公司，他们开始向这些公司提供税收方面的政策激励。

6）灵活的工作时间：如果你是21世纪的父母、学生或者游戏爱好者，这个收益的诱惑是巨大的。假设你需要在周一、周三带孩子去学校，而在周二、周四接他们回来；或者你需要利用上午的某些时间来学习；或者你想在晚上和工会的会友们一起在魔兽世界里比赛。那么，如果能找到一个对工作时间要求比较灵活的公司，你会在工作和生活中如鱼得水。

7）工作现场的益处：虽然，公司可能并不是由于所谓的慷慨大方而向员工提供更多的工作现场激励，但是事实上，这些被激励的员工不但变得更快乐，也更少会为了实现自我而选择另攀高枝。确定你所选择的好处是实实在在的，而不是那些很酷的只能用于吹嘘的噱头。公司是否拥有运动场馆？它是否举办健身班？如果公司并不能提供运动场馆，它是否提供了公司外的其他运动场馆的折扣券呢？或者它允许你报销部分健身费用（一般是50%）？

- 公司是否在员工健康方面关注甚少，甚至没有？
- 对那些有孩子的员工而言，公司是否提供儿童教育的赞助？公司是否提供热食的自助餐厅？食品质量怎么样？是免费的吗？是否有我们喜欢的糖和威士忌？当然啦，自动贩卖

机不在我们的考虑范围。

- 公司是否提供公用的冰箱，提供免费的健康饮品，能让你补充维他命C和其他的营养？
- 公司是否拥有乒乓球桌、空中曲棍球或者其他的娱乐活动？
- 你能否带孩子去公司？时间上有限制么？狗呢？
- 公司是否提供充足的免费停车场？如果公司的地址在某些地价很高的区域，员工可能需要承担部分停车费用，也许公司会转而提供员工的交通补贴。
- 你是否对上班充满向往？办公场所是灰暗无聊还是充满乐趣？你的办公室是在昏暗的、潮湿的、有霉味的一楼，还是在楼宇高层，有很大的窗户和不错的窗外风光？

8）折扣与会员卡：我现在的公司会提供一些大商场的会员卡，还提供那些我们常光顾的小零售商的折扣，一般在15%～20%之间。这些累积起来，可不是一个小数目。

9）金融服务：公司里是否有ATM或者银行？它是否向员工提供信用卡的会员资格或者其他的理财方式？这可以节省你的时间、汽油和金钱。

10）其他：公司还可以提供一些其他的益处。这些公司会非常乐于宣传它们的企业文化，所以，放心大胆地问他们吧。

1.3.2 有形收益

下面所列举的收益可以定量分析，意味着当你对比考虑不同的工作时，可以用美元来衡量这些收益的价值。

1）带薪休假（Paid Time Off，PTO）：假期包括正常的假期、事假和病假。现在，很多雇主更喜欢给员工一些时间，让他们自由安排。如果你有孩子，那么病假是你最期望可以随时获取的。当然，我们不是讨论你自己的病假，而是为了能给你孩子生病时腾出时间，有时候既使你生病了也必须坚持上班。如果你和雇主讨论带薪休假的时候，你雇主更倾向于提供超乎寻常的高额薪水来换取你的休假，那么在你们讨论每小时的报酬之前，请确保你已经计算过3～4周的带薪假和健康保险的价值。

2）医疗保险：确保你比较了这些保险的主要内容，尤其是它们的保险范围和非保险范围。一个公司提供的薪水可能比另一个高5 000美元，但是，可能会要求你承担更多的用现金支付的医疗费用。如果你有家庭或者正打算建立一个家庭，医疗保险就是必不可少的。你现在的医生是否在公司的医生名单上？你是否需要重新找一个医生？这可是一件很麻烦的事。

要明白优先提供者组织（Preferred Provider Organization，PPO）和健康维护组织（Health Maintenance Organization，HMO）的区别。对优先提供者组织保险客户而言，现金支付会有很大的差别，如果你使用弹性开支计划，要预算每月从工资中扣除多少钱是很难的。在传统的PPO下，你通常要为就医或配药先支付10～20美元的费用，再支付你年度就医开支的0～30%（这依赖于你的选择）。它的好处是，你可以看任何医生或者专家门诊，不用和那些推荐的医生预约。与PPO相比，HMO的医疗保险在较小的保险额度的上为所有的实际开支投了保。不足之处在于，你只能看那些它推荐的医生，否则你可能需要自己买单。

仅仅医疗保险是不够的，不要忘了牙齿保健和视力。你还需要了解公伤和非公伤的范围，并确定你现在的医生是否在其名单上。查看提供健康保险的机构所在地，确定你能够在你的住