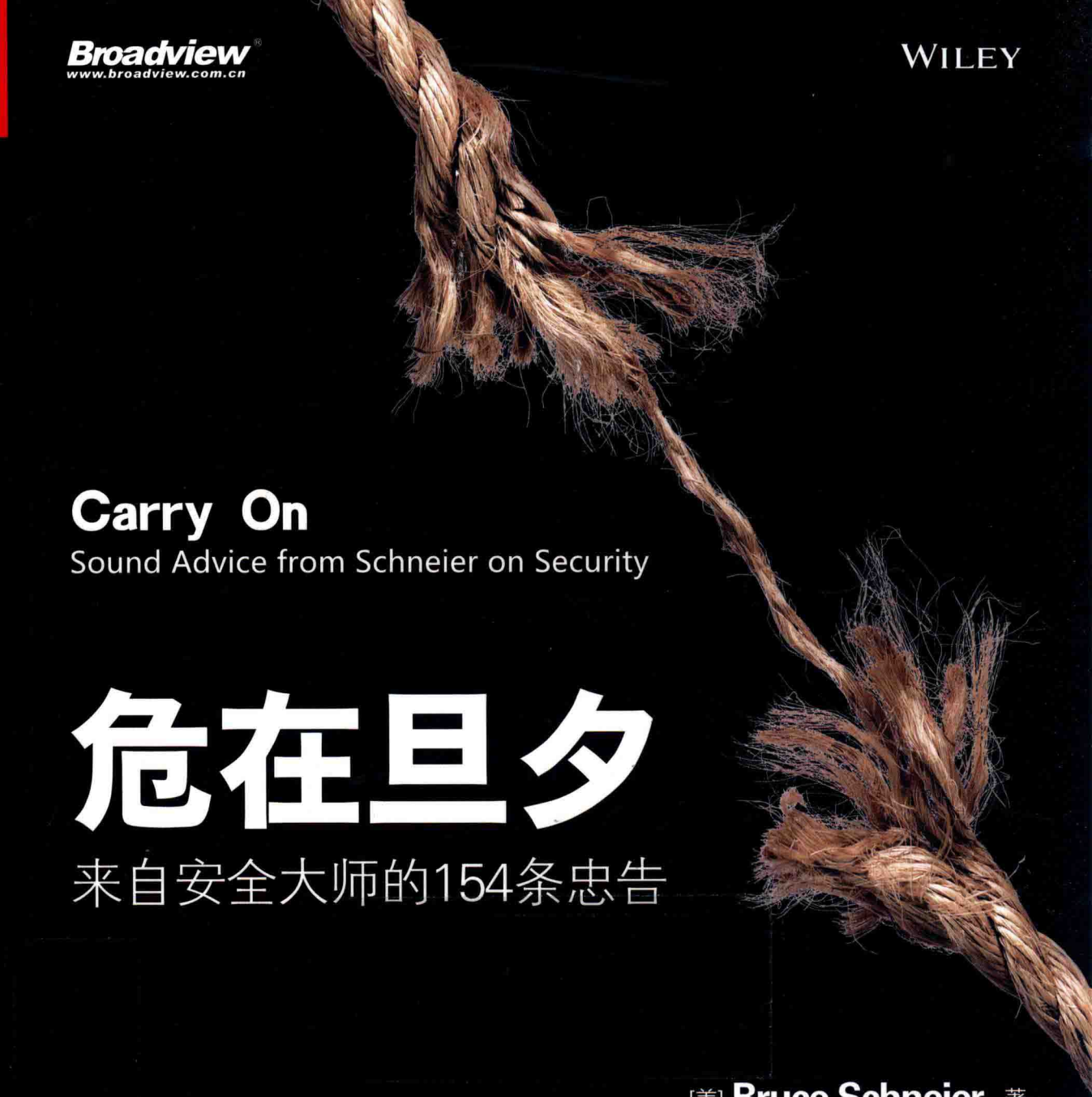
Broadview
www.broadview.com.cn

WILEY



Carry On

Sound Advice from Schneier on Security

危在旦夕

来自安全大师的154条忠告

[美] Bruce Schneier 著

徐菲 王艳 戴士剑 译

中国工信出版集团

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

Carry On

Sound Advice from Schneier on Security

危在旦夕

来自安全大师的154条忠告

[美] Bruce Schneier 著

徐菲 王艳 戴士剑 译

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内容简介

根据 Bruce 的观点，复杂的计算机系统始终存在可被攻击的弱点，软件、系统、硬件设施、人、企业活动等都是构建安全系统的要素。本书分为 8 章，分别从技术、心理、政策等不同的角度分析了安全的特点。Bruce 的见解独到、观点深刻、文笔精湛，影响了全球的安全研究者与实践者，只要你的喜好中包含安全，此书就值得你阅读。

版权贸易合同登记号　图字：01-2015-4170

图书在版编目（CIP）数据

危在旦夕：来自安全大师的 154 条忠告/（美）施奈德（Schneier,B.）著；徐菲，王艳，戴士剑译.
—北京：电子工业出版社，2016.4
书名原文：Carry On: Sound Advice from Schneier on Security
ISBN 978-7-121-28217-1
I. ① 危…II. ① 施… ② 徐… ③ 王… ④ 戴…III. ① 计算机安全 IV. ① TP309

中国版本图书馆 CIP 数据核字（2016）第 039718 号

策划编辑：张春雨　刘　芸
责任编辑：刘　舫
印　　刷：三河市双峰印刷装订有限公司
装　　订：三河市双峰印刷装订有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：787×980　1/16　　印张：17　字数：373 千字
版　　次：2016 年 4 月第 1 版
印　　次：2016 年 4 月第 1 次印刷
定　　价：69.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

引言

我喜欢写短评。我喜欢短评的长度：600 到 1200 字的字数是我最喜爱的；我喜欢短评的格式：用一个严格的论据来证明一个特定的观点；而且，我喜欢短评的风格：我擅长向大众解释复杂的话题。写一本书通常需要付出更多，不仅仅篇幅更长，写书所花费的时间也更长。而短评不同，我可以在一个灵感到来的清晨完成一篇短评，并且顺利的话第二天就能发表出去。

当然，并不是每次都那么顺利。一些短评比较难写，一些十分难写。我喜欢在写一个话题之前考虑几天，也就意味着在发生了一个新事件之后，我通常不会第一时间做出评论。编辑们当然痛恨这一点，他们渴望得到一些能跟上最新动态的东西。

但是写作还是我所擅长的事情，也是我一直在做的事情。自从 1992 年以来，我为各种出版物撰写了大约 500 篇短评、专栏和文章。这些文字都可以从我的网站——www.schneier.com 上找到——这些文字也被整理成两部著作。第一部著作 *Schneier on Security* 中涵盖了自 2002 年 4 月至 2008 年 2 月的作品。而本部著作包含了自 2008 年 3 月至 2013 年 6 月的作品。

整体回顾一下我的作品，我有一些经验、一些观察，以及对于想要出版自己作品的人的一些忠告。虽然我的作品主要与安全有关，但这些建议大多数都是通用的。

- **观点是廉价的。**Charles McCabe 的名言提到“任何呆子都能够认识事实，但是提出观点是一门艺术”。他的说法是正确的，但是却并不意味着所有呆子都没有观点。在互联网上，到处都是各种各样的观点。我很少能够从写短评中获得报酬。不过有几年 *Wired* 付钱请我为他们撰写一个专栏，那是一段有趣的时光，不过最后他们也意识到没必要为我付钱，因为不管怎样我都会继续写作。并不是说把想法写出来赚钱不可能——当然是可能的——只是现在越来越难，越来越少见。

- **说服别人是很困难——也很少见的。**我的目标是撰写有说服力的短评，但是我怀疑这些短评能不能实际上说服别人。通常是，那些已经认同我的观点的人在阅读我的文章，他们试图用一些新的方式理解问题，或者发现一些新的说服别人的说辞。
- **很难不重复自己的观点。**我为不同的读者撰写，通常又是关于类似的话题。我常常重复自己的观点。如果我喜欢一个句子，我会重复使用。如果对于一个话题有一段很好的说法，我也会重复使用。我曾经半业余地写餐馆评论，我常常会抱怨用来表达“这个很好吃”的方法多么贫乏。在我的安全类文章中，这个问题并不严重，但是有时还是觉得表达方式不够用。
- **故事在重复。**一次又一次，我 5 年或者 10 年前撰写的短评，又与一些新事件有关。我 2001 年撰写的关于数据挖掘的文章，在波士顿马拉松爆炸案发生之后又变得重要。1998 年撰写的关于指纹扫描的文章，在苹果公司发布带有指纹扫描的 iPhone 时又引起讨论。2008 年撰写的关于某国网络攻击的文章，自从发表之后，隔段时间就被提起。体育运动中的药物检测、TSA 安全、隐私的价值、无处不在的监控，以及针对个人枪击犯罪的安全，这些话题都一次又一次地在新闻事件中得到关注。有时候我找出一篇旧文章，加入一些新的介绍信息，然后重新发表。不过大多数时候我都会尝试找到一个新观点。我不喜欢重复旧事情，即使这些事情又变成新的。
- **编辑的改编。**有些时候他们只是稍微改编一下，但是大多数情况下他们改动很多地方。有些时候他们的改动是对文章的提高，但是有些时候他们的改动只是让文章变得不同。可以拒绝对文章没有提高的改编。有一次我拒绝一个出版商发表我的文章，因为他们对内容做了太多更改，而且拒绝改回原样。在编辑改动太大的时候，有时候我甚至希望撤回我的稿件。
- **标题不是你的问题。**标题并不是由评论作者来决定。如果比较幸运，你能够在出版前知道标题，但是很可能不知道。标题是出版商吸引读者阅读你文章的媒介。因此，标题通常比你认为的更加情绪化，或者更加简单，缺乏描述。随他去吧——你无法改变这一点。
- **链接会失效。**这很让人沮丧，链接会失效。文章中包含的一些链接，可能一段时间之后再去访问，会返回一个“页面无效”的错误。在我上一部短评集中，我在最后包含了大量链接。我也打算在这本书中这样做，但是检查链接的时候，发现几乎十分之一的链接都已经失效了。其实这些文章并不久远，最远的不过是 6 年前的文章，最新的是最近撰写的。

- **难免犯错。**不要害怕承认错误。如果你是对一些实时发生的事情写一些评论，你的文字中有时候会出现一些错误——关于事实、逻辑、结论、观点的——几乎所有事情都有可能出错。出现错误时，承认这些错误。不要推诿，不要找借口，承认犯了错，你会感觉更好，而且你的读者也会更加尊重你。
- **观点也会改变。**不要害怕你想法的改变。如果你写的东西是关于持续很久的事情的，你的想法可能会改变。可能你发现了新的事实，使得你得出不同的结论。可能你会从新角度思考问题，因此得出不同的结论。这不是问题，只要解释清楚就可以。John Maynard Keynes 曾经说过："当事实改变时，我改变我的观点，先生，您呢?"千真万确。
- **你写的要能够被读者读到。**世界上充满了很多有好想法的人，但是他们从来不把这些想法写出来扩散出去。我对于写作的第一条原则就是，如果不先写出来，就没办法改进。因此，先写出第一个版本。这真的是唯一的方法，能让你意识到你论证中薄弱的部分。（世界上也有很多把糟糕的想法扩散给大家的人，但这是另外一个问题。）
- **试读的读者很重要。**积累一些稳定的试读读者。在文章发表前，找越多的人进行试读，你的文章就会写得越好。不要害怕批评。把你的自尊心从写作中驱离出去，这是接受批评的关键一点。然后试着去理解并利用这些评论。不能让你的自尊心干扰你理解试读读者给出的评论。我是这样认为的，不管怎样，大家总会批评我的作品，如果是在草稿阶段批评，我还有机会在出版前进行修改。几乎我的所有作品在早期的草稿阶段都得到过读者的评论，并依据评论做了修改和提高。如果没有这些修改和提高，我的一些作品可能会十分糟糕。

在撰写一本书的时候，感谢那些阅读并提出评论的人很容易。但如果是短评，就不可能像写书一样。因此在这里，在这本短评集中，我感谢所有曾经对我的短评文稿提出意见的人：David M. Perry, Greg Guerin, Steve Bass, Bill Herdle, David Prentiss, Vicki Laidler, Stephen Leigh, Moshe Yudkowsky, Jon Callas, Doug Whiting, Stefan Lucks 以及 Jesse Walker。如果我不小心漏掉了哪位的名字，在此进行道歉。我没有做记录记下每个人，我知道我也没有记住每一个人。

最后，欢迎阅读我的第二部短评集。我想，每个人在这里都能够根据自己的喜好学到一些东西，只要是喜好中包含安全：技术和安全，经济和安全，心理和安全，政治和安全。我会继续写作，并且可能在 5 年或者几年之后出版第三部短评集。感谢你的阅读。

Bruce Schneier

目录

第1章

商业与经济安全

整合：灾祸还是进步

Information Security

2008 年 3 月

这篇文章是作者与 Marcus Ranum 对话的后半部分。

我们知道，我们不喜欢购买整合的产品套集：一个优秀的产品，同时捆绑了一系列平庸的产品。并且我们也不喜欢购买单项优势产品：很多个提供商，很多个接口，很多个产品，产品之间互不兼容。安全产业一直在这两类方案之间来回往复，新一代的 IT 安全专业人士重复地遇到这两类方案带来的困扰。

真正的事实是这两类方案都不可行。我们不断地欺骗自己，让自己相信目前没有的总是优于已经存在的。实际上，真正的解决方法是购买结果，而不是产品。

诚实地讲，没有人愿意去购买 IT 安全。大家希望购买自己想要的东西，如连接性、Web 展示、E-mail、网络应用等，并且希望所购买的东西是安全的。因此不得不花钱购买 IT 安全只是计算机产业初期的一种假象，需要购买“安全”的情况迟早将会消失。

消失的原因是 IT 提供商们已经开始意识到，安全必须成为产品的一部分。同时，机构已经开始购买服务而不是产品，并开始要求安全成为服务的一部分。安全这一类客户产品将会消失，安全产业将进入 IT 产业。

这里的一个关键驱动因素是业务外包。业务外包是终极的整合，客户在业务外包时不再关心细节。假如我从一家大型 IT 基础设施公司购买网络服务，我不关心它是通过安装最新的入侵检测系统来保证安全，还是通过配置路由器和服务器来实现基于网络的安全。我只想签订一个合同，明确所需服务的等级和质量，其他的事情就交给服务提供商。

IT 就是基础设施，基础设施是一类外包业务。有关基础设施如何运行的细节应由提供基础设施的公司来负责。

这就是 IT 的未来。当这个未来变成现实时，我们将会看到一类我们从未见过的整合。这种整合不再是大型安全公司吞并小型安全公司，而是大型安全公司和小型安全公司都将被非安全类公司吞并。这样的事情已经开始发生，2006 年，IBM 收购了 ISS（美国互联网安全系统有限公司的简称）。同一年，BT（英国电信）收购了我本人的公司 Counterpane，去年该公司又收购了 INS（环球 IT 咨询服务及方案供应商的简称）。这些例子都不再是大型安全公司收购小型安全公司，而是非安全类公司收购大型和小型安全公司。

如果我是 Symantec 和 McAfee 等安全公司的负责人，我会准备好公司被其他公司收购。

这是一种良性整合。这样就不用继续在一个并不是很优秀的产品集和一系列并不兼容的单项优势产品之间做选择，可以完全忽略这个问题。我们可以找一个基础设施提供商，由他来解决安全问题——谁还在意是如何解决的？

预测：RSA 会议规模将如同泄了气的气球般缩减

Wired News

2008 年 4 月 17 日

上周是全球最大规模的信息安全大会——RSA 会议的举办之日。超过 17,000 人齐聚旧金山茅斯考恩中心，在这里听了超过 250 场演讲，参加了数不清的聚会，并且还要躲开 350 多家参展公司的产品推销。

然而，对参展公司来说，最大的困扰是参会人员并不购买产品。

问题不在于产品的质量。展厅中挤满了新的安全产品、新的技术和新的想法，使用这些产品能够从各种不同的方面加强公司的安全。问题在于大多数参与 RSA 大会的人并不理解这些产品的功能，或者说不了解为什么需要购买这些产品，因此他们选择不买。

其中一位来自一家小型安全公司的参会人员购买了一份产品，作为第一个购买的顾客，卖家自豪地邀请他在媒体面前露面。我问他有没有对展厅内的其他同类公司的产品进行比较，寻找性能更优的产品。

他回答说：我实在弄不明白这些公司都是做什么的。

我相信他说的话。展位前堆满了产品介绍，里面充满毫无意义的安全信息，以及不高明的营销文字。你可以走到一个展位前，听销售人员给你做五分钟的介绍，但之后你还是不明白这个公司是做什么的。即使是经验丰富的安全领域专业人士也会感到困惑。

商业需要买方和卖方之间思想的对话，但是对话并没有发生。销售人员无法向购买者解释他们在销售什么，购买者因为不明白销售人员销售什么而无法购买。这两者之间出现了一道鸿沟。他们之间的距离是如此遥远，以致他们甚至不明白对方的语言。

从短期看这是一件坏事，一些优秀的公司将会倒闭，一些优秀的安全技术得不到实施，但从长远看这是一件好事。这体现了计算机行业的成熟过程，IT 正在变得更加复杂和细致，用户正慢慢将 IT 看作基础设施。

我已经预测到安全行业的消亡。当然并不是指信息安全作为一个需求会消失，而是指在 RSA 会议中聚集的用户终端安全行业的消亡。当一类事物成为基础设施时，如同电、水、清洁服务、税务等，用户将不再关注细节，而只关注结果。技术创新变成基础设施提供者需要关注的问题，需要将其打包给用户。

没有人希望购买安全，他们希望购买一些更有用的东西，如数据库管理系统、Web 2.0 协作工具、公司范围的网络等，他们希望这些东西安全。他们并不希望自己变成 IT 安全专家，不希望必须参加 RSA 大会，这就是 IT 安全的未来。

我们可以从公司签订的大型 IT 外包合同中发现，这些合同并不是安全外包合同，而是包含安全的更加通用的 IT 合同。我们可以从现在的产业整合中看到，并不是大型安全公司收购小型安全公司，而是非安全类公司收购安全类公司。我们还可以从流行的软件即服务中看到，用户想要的是解决方案，才不会关心细节。

想象一下，如果防抱死系统——或者任何汽车安全或安全特征——的发明者，需要将防抱死系统直接销售给用户。要想说服普通司机安装该系统，需要做一场艰难的斗争。或许防抱死技术能够成功，也可能失败，但这并不是已发生的事情。防抱死系统、安全气囊以及在车接近其他物体时不断嗡鸣的信号等，都直接销售给了汽车公司，由汽车公司将这些功能结合在一起销售给客户。这并不意味着汽车安全并不重要，而是通常这些新的技术通过汽车生产商来销售。

当然，由于安全的重要性，RSA 会议并不会消失。还会有新的技术、新的产品以及新公司不断出现。但是 RSA 将会转成面向内部，慢慢变成行业会议。安全产品将会变成由安全公司向其他公司销售，其他公司再向企业和家庭用户销售。RSA 将不再是一个有 17,000 个用户参加的会议。

如何销售安全

CIO

2008 年 5 月 26 日

销售界的一个常识是，销售客户想要的产品，比销售——客户为了避免一件事发生而需要的防护产品——要容易得多。人们不喜欢购买保险，或者家庭安全装置，或者计算机安全。并不是说他们不会购买这些东西，只是说服他们购买十分艰难。

原因是心理学上的。当一个安全提供商试图销售产品或服务，一个 CIO 试图说服高级经理投资购买安全产品，或者一个安全人员为公司的员工部署安全策略时，都会遇到同样的问题。

另外一个销售界常识是，我们越了解客户，就越容易销售产品。

人们为何甘冒风险

首先这涉及一点前景理论，这是近来相当热门的行为经济学的基础理论。前景理论是卡尼曼和特韦斯基在 1979 年提出的（卡尼曼后来由于前景理论和其他相关工作获得了诺贝尔奖）。该理论解释了人们在面对风险时，会如何做出抉择。在此研究之前，经济学家提出的经济人模式，认为一位充满理性的人会依据一些逻辑计算而做出抉择。卡尼曼和特韦斯基则让大家了解到，真正的人类行为不仅更微妙难测，也更加难缠。

接下来，我们便做个实验来说明前景理论。将房间里的人分成两组，要求其中一组从以下两个选项中选出一项：100% 的几率获得 500 美元，以及 50% 的几率获得 1000 美元；另外，要求另一组从以下两个选项中选出一项：100% 的几率损失 500 美元，以及 50% 的几率损失 1000 美元。

这两个选择十分类似，但传统的经济学家会认为，人在面对收益或损失时并没有不同：人们是以直接明了的方式计算出相对结果，再据以做出抉择的。有些人偏好 100% 确定的东西，有些人则偏好碰碰运气。无论结果是获得或损失，都不至于影响数学运算法则，当然也就不会影响结果了。这就是传统经济学里的效用理论。