计算机安全技术丛书

信息安全管理之道

[美] Mark Osborne 编著

周广辉 等译

与业内知名专家的直接对话，
本书作者曾保护过白金汉宫的信息安全，
并且管理过KPMG的安全实践。

- 策略和战略的设计与实施
- 理解电子商务和DMZ基础设施的设计缺陷
- 讨论渗透测试和审计报告

中国水利水电出版社
www.waterpub.com.cn

计算机安全技术丛书

信息安全管理之道

[美] Mark Osborne 编著

周广辉 等译

中国水利水电出版社

内 容 提 要

本书是一本信息安全管理的实战指南。全书从介绍信息安全的组织机构开始，对信息安全的原理、概念、法律法规和标准以及审核进行了全面介绍，并结合各种实际经验进行分析，深入介绍了信息安全管理的切实方法。全书共分 13 章，首先介绍了信息安全组织机构、策略、概念、法规和标准，然后以作者实际经历为例介绍了信息安全职位的面试和职员情况，最后全面介绍了信息安全管理所用工具的原理、使用方法以及各种安全测试方法。

本书通俗易懂，实例丰富，并且提供了作者的大量实际经验，不但是一本适合信息安全专业人士使用的实战指南，而且是一本适合各类关注信息安全的人士阅读的参考读物。

北京市版权局著作权合同登记号：图字 01-2006-7278

图书在版编目（CIP）数据

信息安全管理之道 /（美）奥斯本（Osborne, M.）编著；周广辉等译. —北京：中国水利水电出版社，2008
（计算机安全技术丛书）
书名原文：How to cheat at Managing Information Security
ISBN 978-7-5084-5023-0

Ⅰ. 信… Ⅱ. ①奥…②周… Ⅲ. 信息系统－安全管理 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2007）第 155134 号

书　　名	信息安全管理之道
作　　者	[美] Mark Osborne　编著
译　　者	周广辉　等译
出版发行	中国水利水电出版社（北京市三里河路 6 号　100044） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）63202266（总机）、68331835（营销中心）、82562819（万水）
经　　售	全国各地新华书店和相关出版物销售网点
排　　版	北京万水电子信息有限公司
印　　刷	北京蓝空印刷厂
规　　格	787mm×1092mm　16 开本　14.5 印张　272 千字
版　　次	2008 年 1 月第 1 版　2008 年 1 月第 1 次印刷
印　　数	0001—4000 册
定　　价	28.00 元

凡购买我社图书，如有缺页、倒页、脱页的，本社营销中心负责调换

关于作者

Mark Osborne 现在是 Interoute Communications Limited 公司的 CISO，该公司是欧洲最大的下一代网络的所有者和运营商。在此之前，他曾担任 KPMG 的安全实践方面的负责人，在 KPMG 工作期间，他建立了 KPMG 的安全团队。这是一项价值几百万英镑的业务，他负责从头开始组建它。尽管该团队不再运作，但它仍然是英国最大、最受尊敬、最盈利的安全团队之一。Mark 自豪地声称，他最伟大的成就之一就是曾经管理过这些高效率的安全专家达六年之久。

他拥有 MBA 和计算机学位，还获得了 CISSP、CISM、CCSP 和 CCSE 认证。他由于指出了许多 WAP 的安全缺陷而广为人知。他也曾经发布过许多零时差漏洞（zero-day vulnerability）和几个 IDS/安全工具。大多数经过认证的道德黑客图书和课程都有三个独立部分介绍他的工作。他的成就包括：

- 1988 年设计和开发了一个安全子系统，该子系统使得流行的 ADABAS 数据库（许多银行和证券交易所使用这种数据库）能够得到领先的安全产品 RACF、ACF2 或 Top-Secret 的保护。该子系统和这些产品一起分发。
- 1995 年参与了两个里程碑式的法律案件；就任一家著名银行的 KPMG 安全专家；在两家主要航空公司之间的 cash-for-rides 行动（Dirty Tricks 运动的延续）中担任计算机安全专家证人。他证明了拥有计算机的乘客名单被滥用，并且促使该案件在英国最终达成了庭外和解。
- 1997～1998 年在英国最早的三家网络银行担任安全顾问，随后为更多的网络银行工作过。后来，他每次讲演都以这样一句话开始：我闯入过的银行比 Jessie James 闯入过的还要多。
- 1998 年着重介绍和宣传 WAP 中的安全缺陷，其中最值得关注的是 WAP Gap。他的许多文章出现在大多数制造商的 Web 站点和大学门户网站上，不过他们忘得实在太快了。
- 2002 年与一家知名的制造商约定进行一系列关于移动商务的安全调查。他们的报告有 40 页，但工作做得非常糟糕，甚至包括利用一家不知名的装饰品供应商进行了一次小型的“驾驶攻击”（war-driving）练习。

  最终结果是，作者进行了英国第一次记录实际的无线多点入侵活动的蜜罐调查，该活动基于入侵行为的公认标准进行。该调查在全球范围内受到了广泛关注，并且成为许多政府资助活动的资料来源。
- 2003 年设计了流行的 WIDZ IDS 和 fatajack 零时差漏洞。

他曾在或曾代表以下公司担任安全经理、安全顾问或安全测试人员：Pru/Egg、Commercial Union、TSB、Lloyds TSB、Co-operative Bank/Smile、Halifax、Barclays、Bank of Scotland、RBS、CSFB、Barclaycard、Yorkshire Bank、Astra Zeneca、Czech National Bank、National Bank of Greece、Merill Lynch、Sakura、Mercedes-Benz、BMW、NatWest、Fuji Bank、

Hiscox Insurance、Nestle、HSBC National Audit Office、DKB Bank、Cheshire Building Society、Alliance and Leicester、Deutsche Bank、British Telecom、Cable & Wireless、TeleWest、EuroBel、AxA Insurance、Churchill Insurance、Esure、Std Chartered Bank、Hill Samuel、NaB、EBRD、BIS、Hayes、DX、various government departments、Lombard Tricity Finance、MBNA、Newcastle Building Society、Woolwich Building Society、Cedel、Singer & Friedlander、BskyB 和 RailTrack。

Mark 也不完全是一个乏味的计算机迷，他的妻子就能忍受他的行为，而他的两个孩子则把他当作一个不负责任的大哥哥。

关于本书的技术编辑

Paul M. Summitt（MCSE、CCNA、MCP+I 和 MCP）拥有大型通信方面的硕士学位。他曾经担任过网络、Exchange 和数据库管理员，也担任过 Web 和应用程序的开发人员。Paul 曾经编著过虚拟现实和 Web 开发方面的书籍，也曾担任过几本关于微软技术的图书的技术编辑。Paul 和他的妻子 Mary（也是他的写作伙伴）居住在密苏里州的哥伦比亚市。

序

有时候我会被询问为什么要写这本书，而我的答案可以总结为一个很简单的故事。在我为一家大型审计公司工作时，一位审计人员曾打电话找我（我好像认识他），他满怀热情地说："您好，下周我要去参加一个安全管理人员职位的面试，我知道那意味着要与密码和黑客打交道，但是您能告诉我一些更详细的东西吗？"

他一定认为我是不小心挂断了电话，因为他打回来两次！

本书不是安全方面最全面的书籍，但我认为它包含许多好的IT安全管理人员应该掌握的内容，它也是我的审计朋友绝不会购买的那种书籍。

信息安全与主流信息技术和其他业务领域的许多其他学科是不同的。虽然现在各个领域都有许多很好的书，但要获得跨多个子领域的知识仍然很困难，而这一点对于一本成功的图书来说至关重要。

安全是一个需要从业者在整个机构中操作的领域，而不像IT那样具有那么多功能。除了某些没有其他替代方案的忠告之外，一位首席信息安全官（CISO）或安全管理人员可能会被要求提供许多安全方面的建议。有时候最好的建议可能是最大的希望。因此，敏感的安全官员努力在大多数领域拥有良好的基础。但遗憾的是，许多人不是依靠知识（通过正规课程或自学获得的）提出建议，而是使用权威的语气、Google搜索或各种关于"安全策略"的定式来发号施令。有些专家看似知道所有东西，但是他们的建议往往有一半需要反过来使用，他们的建议经常会导致项目延迟甚至罚款，浪费公司几十万英磅的费用。

本书基于作者极其丰富的实际经验编写而成。作为安全方面的专业人士，作者曾经在安全机构中最高和（可能是）最低的层次中工作过。这为作者提供了一个全面的视角，这种视角可能与其他许多图书不一样，但是它能够帮助你摆正自己的观点。例如，当一些技术人员夸大防火墙的功能时，你可以使用从本书获得的知识让他们修正自己的观点。

本书的每一章都以作者的"实际经验"作为开始，内容简明扼要，但又能够为读者提供一些重要的信息。

作者试图通过本书解释"我们为什么要这样工作"这个问题。我不知道这是否是因为我比较聪明，也许是因为我年长一些，在人们还正在试图解决这个问题时，我已经得到了答案。

※　　※　　※

本书由周广辉翻译，在翻译过程中，得到了安晓梅、易磊、欧阳宇、张波、盛海燕、徐红霞的帮助，其中安晓梅审校了全文。在此一并致谢。

目　　录

第 1 章　信息安全的组织机构

本章目标：

- 评估信息安全职能的典型职位以及各种职位的优点。
- 定义安全职能的角色。
- 讨论一个好的 CISO 应具有的品质。

1.1　轶事

作为一名首席信息安全官（CISO），必须能够向雇主展示某些关键品质。在我最近一个职位的面试中，当我坐下时我错误地估计了位置，椅子扶手正好插进我的裤兜并发出了撕裂的声音。我的高级顾问套装现在完全具有空气调节功能了。

我立刻宣布："我弄破了我的裤子。"这样我的面试官就会知道这声音的确切来源，很明显它是从我的座位上发出来的。然后我说："现在你可以了解到我没有瞎说。"

这就是经验！

1.2　引言

没有任何两个组织机构是相同的，它们各自拥有不同的文化、规模、行业领域和职员。因此，下面这个问题没有所谓的正确答案（但可能会有许多错误答案）："应该怎样定位一个组织机构中的信息安全负责人和信息安全团队？"将信息安全负责人和安全操作团队分开经常是一个有目的的商业决策。

本章探讨了各种规模的组织机构如何设立它们的信息安全职能的问题。本章基于我 10 年安全领域工作经验中的观察进行探讨，而我这 10 年的工作主要是为英国主要的、有钱的公司提供战略和技术细节层面的安全咨询。

据我所知，没有其他任何一本书籍或手册讨论过该主题。

1.2.1 信息安全团队的位置

图 1.1 所示为一个典型公司的员工体系，它包含了安全职能的一些可能的位置。本章将分析对每个可能位置的赞成及反对观点来回答那个古老的问题：“信息安全应该处于什么位置？”

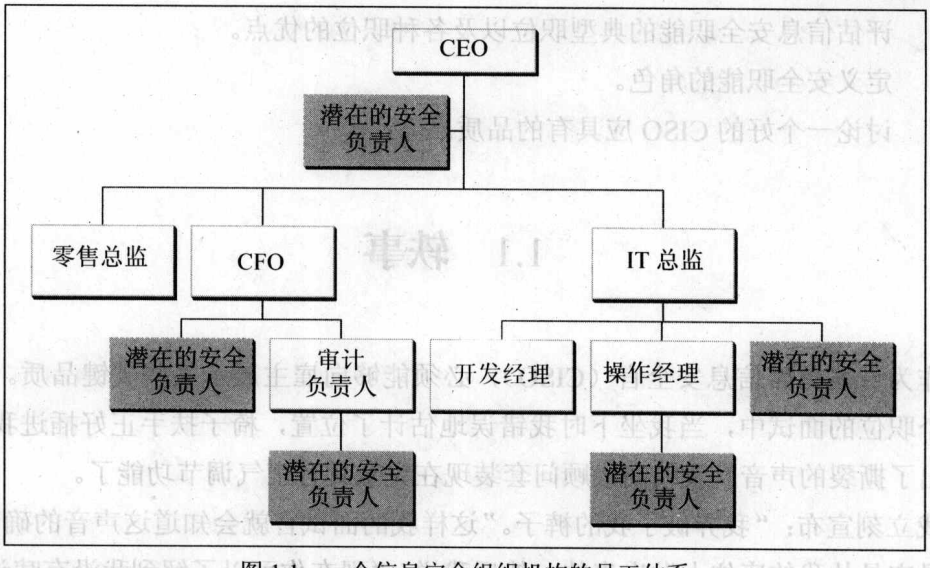

图 1.1 一个信息安全组织机构的员工体系

1.2.2 信息安全的位置：通过 IT 总监向上汇报

对于 CISO 和安全职能来说，它们最常见的位置是通过 IT 总监或计算机操作部门的负责人向上报告。当然，后者的结构在小公司中比较常见，这些小公司对信息安全没有法规方面的要求。如果公司被监管，或者甚至在交易所中上市，权力机构可能会要求将信息安全设立在一个较高的位置。奇怪的是在有远见的公司中这种情况也很常见，这些公司拥有安全团队的历史已经有 20 年。这可能是因为安全团队是由资源访问控制设备（Resource Access Control Facility，RACF）管理员的可靠团队发展而来的（RACF 是 IBM 主机上的一种安全软件）。

访问具有这种结构的组织，就可以在很短的时间内认识到这种定位的优点和缺点。

1. 优点

将安全团队定位在 IT 总监报告范围内的优点包括：

- 在进行 IT 决策时，信息安全职能不会受到很多“外行人”的阻挠，因为它是计算机部门的一部分，所以它不会受到“外部”干涉。
- 操作性的计算机安全任务（安装防火墙、设置路由器访问列表或其他类似工作）将会由该团队来执行，而不是制作一个规格书后由其他团队执行。作为结果，该团队将成为公认的本地专家。
- 让技术安全职员能够专门研究某个领域，并且与其他技术领域紧密合作。在这个过程中不仅仅只有技术的交流，职员之间的关系通常也会变得更好。

2. 缺点

将安全团队定位在 IT 总监报告范围内的缺点包括：

- 信息安全的声音不是那么强有力。
- 信息安全可能面临资金不足的问题。
- 信息安全不独立，它总是被认为是 IT 部门最容易的工作之一。典型情况下，由于信息安全职位较低以及其属于 IT 部门这个事实，其工作重点往往倾向于计算机安全而不是信息安全。业务风险和评估损失及影响的结构技术不会起关键作用。

显然，在某种情况下，这种定位不是一个大缺点。英国最大的银行之一恰恰是以这种方式组织其安全团队的。但是，当您直接汇报给一个负责 5000 人的 IT 总监，而同时超过 100 个信息安全职员向您进行汇报时，您可能不会感觉您的决定缺乏力量。类似地，如果一个组织机构几乎所有的问题都集中在 IT 部门，而 IT 是核心业务（例如一个互联网公司），这种定位将是一个重要的优点。

然而，在这种规划中通常不会有完善的风险管理。这种角色范围允许安全职能有效地管理数字和计算机安全，但对于非数字资产的信息风险管理的影响充其量只能作建议。这个事实有时具有严重的缺点（例如在纸质文件的安全方面），但现在计算机环境非常普及，因此这种定位的影响还是相当大的。就像后面章节中所讨论的那样，充分与其他部门合作会在相当程度上减少这种缺点。

1.2.3　信息安全的位置：向审计负责人汇报

另一个并不太理想的安全团队的位置是让其汇报给审计职能的负责人。以我的经验，当安全团队由计算机部门的子部门成长起来并具有一定规模后，它经常被这样设置。

但是我保证，您绝不希望与审计人员协同工作。

1. 优点

将安全团队定位在审计职能的负责人下面的优点包括：

- 团队独立于计算机部门。
- 团队将会得益于审计部门对于整个企业的管辖权。如果审计团队成员由于共享密码而被抓住，他们将不能再以那是 IT 部门的事情作为借口。
- 老板（审计部门的负责人）将要求采取一种全盘的信息安全步骤，而不是仅仅实施计算机安全。
- 安全团队会拥有强大的朋友，如管制机构或审计委员会。

2. 缺点

将安全团队置于审计职能的负责人下面的缺点包括：

- 没有人愿意见到一个审计人员。团队趋向于被当作判断者和反应者，而不是主动的修理者或问题解决者。
- 审计人员通常是杂而不精，他们一般不会在技术层面努力做自己的工作。小组将永远不会被认为是一某个方面问题的专家。

1.2.4 信息安全的位置：向 CEO、CTO 或 CFO 汇报

将安全团队置于 CEO、CTO 或 CFO 之下是最好的解决方法。这种汇报位置确保了其他部门能够充分注意您的发现，而且它还独立于任何操作性的部门。

1. 优点

将安全团队定位在 CEO/CTO/CFO 下面的优点包括：

- 赋予了安全团队一定的权力。
- 具有独立性。
- 位置足够高，因此具有整个企业的视角。
- 它向所有人表明了组织非常严肃地对待安全问题。

2. 缺点

将安全团队定位在 CEO/CTO/CFO 下面的缺点包括：

- 安全小组会被指责呆在象牙塔里面（那又怎样？）。
- 安全团队将会发现很难窥视 IT 总监的业务活动和部门。