HZ BOOKS 华章经管

WILEY

MCKINSEY COLLEGE 麦肯锡学院

# 麦肯锡的数字业务安全策略


[美] 詹姆斯 M.卡普兰（James M.Kaplan）
图克·拜莱（Tucker Bailey）
德里克·奥哈洛伦（Derek O'Halloran）
阿兰·马库斯（Alan Marcus）
克里斯·雷策克（Chris Rezek）
著

班晓芳 佟鑫 译

麦肯锡顶级信息安全专家
护航全球数字化所创造的数十万亿美元经济价值

# BEYOND CYBERSECURITY

PROTECTING YOUR DIGITAL BUSINESS

机械工业出版社
China Machine Press

MCKINSEY COLLEGE 麦肯锡学院

# 麦肯锡的数字业务安全策略

詹姆斯 M.卡普兰（James M.Kaplan）
图克·拜莱（Tucker Bailey）
[美] 德里克·奥哈洛伦（Derek O'Halloran） 著 班晓芳 佟鑫 译
阿兰·马库斯（Alan Marcus）
克里斯·雷策克（Chris Rezek）

BEYOND CYBERSECURITY
PROTECTING YOUR DIGITAL BUSINESS

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

麦肯锡的数字业务安全策略 /（美）詹姆斯 M. 卡普兰（James M. Kaplan）等著；班晓芳，佟鑫译 . —北京：机械工业出版社，2016.10
（麦肯锡学院）
书名原文：Beyond Cybersecurity：Protecting Your Digital Business

ISBN 978-7-111-54921-5

I. 麦… II. ① 詹… ② 班… ③ 佟… III. 互联网络－网络安全－安全技术
IV. TP393.408

中国版本图书馆 CIP 数据核字（2016）第 229620 号

本书版权登记号：图字：01-2016-2382



# 麦肯锡的数字业务安全策略

出版发行：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：王金强　方　琳　　责任校对：殷　虹
印　　刷：北京诚信伟业印刷有限公司　　版　　次：2016 年 11 月第 1 版第 1 次印刷
开　　本：170mm × 242mm　1/16　　印　　张：15
书　　号：ISBN 978-7-111-54921-5　　定　　价：45.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）68995261　88361066　　投稿热线：（010）88379007
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjg@hzbook.com

我们正处于一个科技创新涌现的时代，沟通、协作以及企业和机构的变革速度十分惊人。然而，在我们的生活、工作日益依赖于科技进步时，也出现了同样惊人的安全风险。如果你经常关注每日的安全漏洞新闻，就会了解科技带来的经济风险、经营风险以及信誉风险。

作者将自己多年的研究成果全部写入本书，详尽解释了当今社会造成很多网络不安全的原因，网络安全为何成为一个极为棘手的问题，问题为什么变得越来越糟糕，以及企业、行业管理部门、政府部门应该采取哪些措施。重要的是，五位作者詹姆斯 M. 卡普兰（James M. Kaplan）、图克·拜莱（Tucker Bailey）、克里斯·雷策克（Chris Rezek）、德里克·奥哈洛伦（Derek O'Halloran）和阿兰·马库斯（Alan Marcus）不仅仅介绍了现今面临的网络安全风险，还详尽描述了如何缓解风险，并评估了如果不采取缓解措施可能导致的危害。

在调研过程中，我有机会了解他们的研究方法及初步结果。他们在全球诸多企业机构看到的事实，与我看到的或者我从 RSA 客户处听到的事情基本一致。在 2014 年 RSA 大会上，作者们将初步研究成果展示给来自欧洲、亚洲、美洲的各国代表，引起了大家的共鸣，一致同意本书所呈现的事实。让我感到振奋的是，会议中所有国家都认为当前大家共同合作解决网络安全问题非常必要。

从研究成果中可以看出，融合了云计算、移动互联网、社交媒体技术的当代数字化商业发展迅速，大幅增加了组织机构的受攻击面，传统的安全边界

（perimeter）不再是有效的防护。过去各机构与外部世界的屏障已被打破，网络边界呈现新的特点，即碎片化、飘忽不定且与内网关联紧密，致使我们原来依赖的安全控制效果大大降低。这就需要新的安全模型。本书作者推荐了一种基于数字化适应力（digital resilience）概念的多层次方法，目前一些世界领先公司已经开始使用，并很快接受了这个方法。

数字化适应力不仅是一种理论，也是一种策略，是在日益不安全的世界里带来真正安全的策略、过程以及控制的框架。首先，需要透过企业的业务目标、发展重点及关键资产，全面理解风险种类以及处理风险的必要性。其次，要在商界领袖群体中创建一种安全文化，使高级管理人员在商业决策时时刻刻想到安全，而非事后才想起安全的重要性。再次，要时刻做好应对任何来源的攻击，包括来自内部的威胁。为了及时应对不可避免的入侵，要采取必要的可视化手段、分析工具及动态控制措施。最后，要将所有这些因素有机地结合起来，创建起真正的深度防御体系。

但是，每个组织机构都不是孤立的岛屿，仅靠自己的努力很难成功抵御风险。作者认识到，这需要政府、监管者、供应商、行业共同组成生态系统，通力合作，形成一个保护生态系统的良好对策。

对于很多组织机构来说，网络安全这一话题仍旧是讳莫如深的，恐惧及绝望感弥漫在很多组织机构。如本书作者在阐述持续的网络安全带来的经济影响时说道，因为恐惧及网络风险的不确定性，阻碍了企业采用创新性、有潜在变革性的技术，因此，由于对网络安全缺乏清晰认识所造成的影响要远超过目前我们面临的挑战。正如两次荣获诺贝尔奖的居里夫人所说："生命中没有可畏惧的东西，它只是尚待理解。我们要更多、更充分地去了解，这样我们就少了畏惧。"

本书作者潜心研究，帮助人们加深这份理解，为读者提供必要的分析，指出了一条非常清晰、有说服力的路径，这条路通往安全的未来。

我相信，本书可以极大地帮助安全从业人员、技术部门主管，不

仅让他们用现实世界的安全防御成果来作为衡量标准，而且，本书作为一种工具，向高层管理人员阐述了网络安全对其所在组织机构的未来以及企业的生存能力都是非常重要的。

政府公务员及行业监管者应将此书视为指南，制定周到、行之有效的政策及切合实际的管理规章，为企业提供更多的安全支持。

最后，本书对于高管及董事会成员来说也颇具价值，可帮助他们很好地理解所有组织机构面临的问题。我经常受邀在组织机构的董事会发言，讲述他们的网络安全现状与前景，在这些对话中，我时常总结自己的经验和世界各地客户的体验，现在，很感谢让我也能在这里与读者分享本书。

亚瑟 W. 科维洛（Arthur W. Coviello, Jr.）
EMC 公司信息安全事业部 RSA 执行总裁

# 前言

未来10年，世界经济的发展进步依赖于数字化创造的数十万亿美元的价值。组织机构已经从拥有小规模自动化的系统，发展成为充分利用无处不在的网络连接、海量分析、低成本、高扩展性的技术平台。技术进步显著增加了不同级别客户的亲密度、业务操作的灵活度及决策者的洞察力。在银行业，这意味着几分钟内即可成功开户、批准按揭，而非几天甚至数周。在保险业，这意味着在大量分析数据的支持下，有更好的保险核保及更公平的价格。在航空及酒店领域，这意味着更高的透明度，为旅客减少一些麻烦。

当“一切都是数字化”时，私营、公共及民间机构就越来越依赖信息系统。当今世界是一个超级关联的世界，在线和移动业务增加了企业的安全脆弱性，企业更容易受到富有经验的网络罪犯、政治激进黑客甚至内部员工的攻击。只有当客户及企业在面临越来越强大的网络攻击时，仍对财务记录、患者数据及知识产权的机密性和可用性的安全保持信心，数字化进程才能成功。

要保持经济的持续发展，必须保护组织结构免受网络攻击的影响。在2014年达沃斯世界经济论坛年会上，论坛组织者与麦肯锡机构联合提出，要提升网络安全在高管中的关注度。我们一致认为，有两方面的关注度至关重要：一是要充分认识到企业遭受网络攻击后的战略影响和经济影响，另一种是要制定企业获得数字化适应力的规划，即规划整个网络安全生态系统中所有参与者应该怎么做，特别注重如何将网络安全作为一个商业问题而非技术问题来解决。

经过采访、调查以及参加由数百个组织机构高管参加的工作会议，我们发现了以下几个问题：

第一，如果组织机构在保护自己的方式以及外部支持方面没有巨大变化，网络攻击风险将降低人们对数字经济的信任和信心，到 2020 年，数字经济所能创造的价值将降低 3 万亿美元。为应对此问题，全球的组织机构需要提升数字化适应力，只有这样，才能从超级关联的世界中获取价值，即使是冒着业务中断、知识产权（IP）流失、声誉损失、网络欺诈等风险。

第二，虽然各公司都一致认识到提升数字化适应力要采取的措施，但并没有尽快落实到位。要提升数字化适应力，公司应将网络安全深度整合到现有业务流程及信息技术（IT）环境中。然而目前大多数公司仍将网络安全视为一种控制功能（control function），这不仅导致保护信息资产的安全需求与数字化进程之间产生冲突，而且还与从技术投资中获取价值的需求发生冲突。即使是最大型、资金最充裕的机构，其网络安全项目也设计得相对落后，它们仅从技术控制入手，而不是控制商业风险，因而没能推动更广泛的组织机构层面和业务流程产生必要的变化。

第三，公司若要提升数字化适应力，需要增强网络安全团队与业务团队之间的协作，让企业 IT 部门更加注重适应性，大幅提升网络安全功能的技能与水平，唯有首席执行官及高级管理层才能推动如此大规模的变革。

除了公司自身，其他组织结构都不可能解救公司于网络攻击，但是监管者、执法机关、国防及安全部门、技术供应商及行业协会等机构能够在一个数字生态系统中起到重要作用，可显著提升公司的数字化适应力。目前人们对公司如何保护自身安全有很多一致性看法和对策，但对于如何建设更广泛的数字生态系统，一致性意见较少。此时公共、私营、非营利机构等之间的相互协作将变得至关重要。

## 建立数字化适应力的前提

在考虑数字化适应力之前，首先要理解网络攻击与网络安全，以

及它们与数字生态系统的关系。

## 网络攻击：面临的多种业务风险

在数字化特征越来越明显的经济社会中，世界上大部分组织机构都依赖着“信息资产”，这些信息资产，有些是结构化数据，有些是非结构化数据，例如客户数据、知识产权、商业计划，以及从客户服务到供应商付款的在线流程。针对这些信息资产的网络攻击，有些是出于攻击者个人炫耀的目的，有些是为了经济利益，而有些则是出于国家政治利益。一般普通老百姓主要关注知识产权侵犯、信用卡数据窃取等信息，但对企业来说，需要考虑更多的潜在风险（见表 0-1）。

表 0-1　企业面临的网络安全风险

| 风险类型 | 攻击发起者 | 攻击目的 |
| --- | --- | --- |
| 竞争力下降 | 外国竞争对手 | 为获得经济利益而窃取机密的商业计划 |
| | 外国情报机构 | 出于国家竞争优势考虑，窃取别国知识产权 |
| | 跳槽到新公司的员工 | 带走客户信息去为竞争对手工作 |
| 违反监管与法律 | 网络犯罪组织 | 窃取客户数据，供日后进行身份盗用或医疗欺诈 |
| 企业名誉损失 | 员工 | 对公司政策不满而公开敏感文件 |
| | 黑客活动分子 | 对公司政策不满而泄露和公开管理层讨论的机密政策 |
| 诈骗与盗窃 | 网络犯罪组织 | 破坏在线金融交易以进行欺诈 |
| | 网络犯罪组织 | 损坏重要信息资产，除非收到赎金 |
| 业务中断 | 恐怖组织 | 改变重要业务流程数据，伤害自己不满意的国家或组织 |
| | 内部人士 | 因为怀疑自己会被炒鱿鱼而破坏企业数据 |
| | 黑客活动分子 | 为引起注意而扰乱业务流程（如在线客户服务） |

## 网络安全：公司如何保护自己

虽然企业面临着经营目标、资源限制、合规性要求等压力，但网络安全[1]仍然是组织机构避免受到网络攻击而应采取的一项业务功能。

它包含三个方面：风险管理功能、影响功能及交付（delivery）功能。

首先，网络安全本质上是风险管理，因为没有办法阻止所有网络攻击的发生。正如一位首席信息安全官（CISO）所说："我的工作不是降低风险，而是让企业能够明智地接受一些风险。"

如果公司打算采用新的客户移动服务平台，就要承担相应的风险。因为新型移动平台给攻击者获取公司数据提供了新途径。但如果公司希望这个平台能提高每个客户的平均收入，那么作为风险管理者，就需要帮助企业领导权衡网络安全风险。CISO 应回答以下问题：

- 采用新型移动平台将带来哪些安全风险，业务经营收益是否能说明安全风险是可接受的。
- 在设计平台时，如何既保证平台业务数据丢失风险降到最低，又保证良好的客户体验（进而产生好的业务影响）。

其次，网络安全工作具有影响作用。CISO 和企业领导共同商讨企业安全风险与投资回报之间的关系后，企业各个部门再采取相应的执行措施：采购团队就安全需求进行谈判并写入合同；管理者必须限制机密文件的分发范围；开发人员要设计安全的应用软件，编写安全的代码。网络安全工作必然涉及大量的利益相关者，其中有些工作需要按照法律法规开展，有些工作则需要采取更为贴合的、更有效果的措施。

最后，网络安全具有交付作用，包括管理防火墙、入侵检测、恶意软件检测、身份管理和准入管理等技术，也要管理一些保护信息资产和在线流程安全的行为，如采集和分析威胁情报、取证分析。

业务功能的网络安全不同于组织机构功能的网络安全。一家公司可能将所有或大部分风险管理、影响及交付活动整合到单一的网络安全团队或分布到几个组织机构里。

## 数字生态系统：公司不能仅靠一己之力保护自己

组织机构首先要保证自己安全，才能为庞大的数字生态系统提供

安全保护（见图 0-1）。数字生态系统包括：

- 企业客户：企业客户连接到企业网络中处理业务增加了便利性，但也增加了企业的安全风险。攻击者可能会利用客户的 IT 环境作为入侵企业网络的途径。同时，企业客户也会担心企业是如何保护自己的数据的。这两种情况对企业安全保护能力提出了更高的要求。
- 零售客户：相对于企业客户，普通消费者对网络风险没有那么敏感，不过，企业保护数据的方式可能已经影响他们的购买决定了。
- 企业供应商：某种情况下，律师事务所、会计师事务所、银行、业务流程外包服务商等供应商将会掌握公司最敏感的数据。考虑到公司网络的互联性，供应商网络也可能成为攻击入口点。

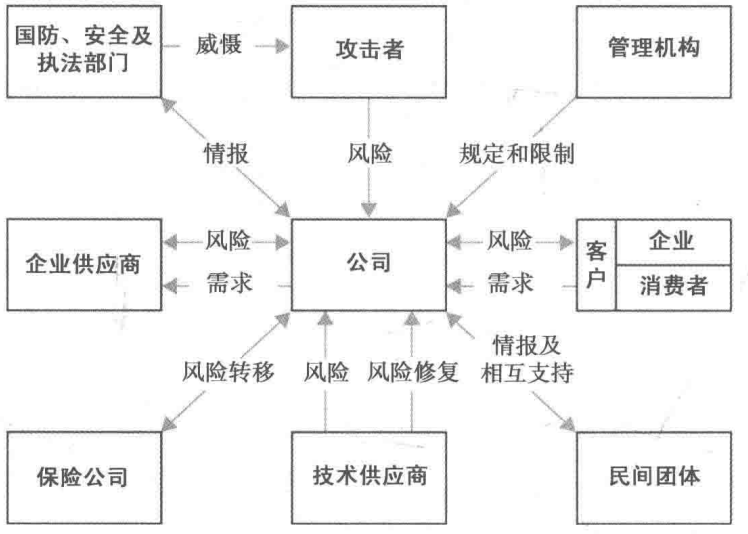


图 0-1　公司面临广泛的网络安全风险

- 技术供应商：供应商既能提供风险控制，但同时也是风险引入源。我们购买的任何技术都可能有安全缺陷，出现让攻击者有机可乘的弱点。技术供应商可提供能让公司降低风险的商品和服务，通过消除漏洞、分析网络攻击等方式降低风险，保护企业的技术环境。

- 政府部门：公共部门在影响网络安全环境中扮演着多重角色，包括调查攻击、起诉攻击者、规范私营公司，有时要求企业采取特别保护措施，批准企业网络安全策略。它们也调整法律、开展安全研究、分享情报或传播安全技术。
- 民间团体：从行业协会到标准制定机构和倡议组织，有大量民间团体参与到数字生态系统中。
- 保险公司：网络保险尚处于早期阶段，但即使在今天，有些保险公司为了换取保险费，愿意承接企业的网络攻击风险。

## 什么是数字化适应力

高管们有时会问首席信息官（CIO）和首席信息安全官（CISO），网络安全何时会得到解决、网络攻击的风险何时能远去、何时能不再为此担心。有时，他们会将这些与民航业务类比。在喷气机时代，会发生一些可怕的事故，现在，航空公司非常注重安全，搭乘出租车前往机场却成为飞机旅行最危险的一个环节。

或许拿开车来比喻网络安全更合适。比起民航出行风险，开车是更多人利用更多车辆从事更为广泛的活动，风险更大。我们可以通过提高最低驾车年龄至 30 岁、限制最高时速 25 英里[⊖]，把机动车事故降至几乎为零，然而如果这样做，这种个人出行交通方式就遭到毁灭性打击。

如果一位银行业 CEO 不用担心市场风险和信用风险，他就绝不会询问有关事情。但他明白他所在的机构是通过接受这些风险来换取有经济收益的业务的，因此，他的业务需要了解市场风险、信用风险以及其他风险，并在有潜在收益的情况下，适当地管理这些风险。

考虑到当前社会数字化程度越来越高，科技创新速度加快，攻击者可能超出执法机关的控制等情况，我们不能期望很快消除网络攻击

⊖ 1 英里＝1 609.344 米。

对世界经济的影响。不过，企业和全球经济体可寄希望于达到数字化适应力的状态，包括：

- 应了解网络攻击的风险，并且能做出恰当的商业决策。通过经济收益证明，不断递增的风险是可以接受的。
- 应坚信网络攻击风险是可以控制的，网络攻击风险不会将公司置于风险高位。
- 消费者与企业应对在线业务有信心——信息资产面临的风险及在线欺诈风险并不会阻碍电子商务的发展。
- 网络攻击风险不会阻碍公司的技术创新步伐。

在这样的背景下，世界经济论坛和麦肯锡咨询公司已经开展合作，了解如何帮助企业与国家都达到自己的安全期望。

## 背景与方法

自 2011 年以来，“超级互联世界中的风险与责任”成为世界经济论坛的一个议题。2012 年年中，该论坛又与近百家公司合作签署了《网络适应力标准》。标准中要求各参与公司承担起义务，要认识到自己在促进弹性数字经济中能够发挥的作用，并制订实用、有效的实施计划。该标准也鼓励高级管理层增强风险意识，提高对网络风险的管理能力，并且在适当的情况下，促使供应商和客户对弹性数字经济具有同样的认识。[2]

2014 年达沃斯世界经济论坛中，麦肯锡受邀对论坛高层管理人员进行辅导，以提升应对网络攻击、网络安全及行业数字化适应力的管理水平，行业不仅局限于技术与通信，还包括金融服务、制造业、生活消费品、交通运输、能源及公营部门。

麦肯锡与该论坛共同认为，该项目的最佳成果是形成了一套网络攻击战略定位和经济定位的真实观点，以及一份计划——网络安全生态系统中的所有参与者都应制订如何实现数字化适应力的计划，更重要的是，让高层管理者将网络安全看作一个业务问题，而非

技术问题。

我们从2013年晚春开始收集数据，在夏、秋季节构思并验证我们的假设，2014年达沃斯世界经济论坛年会上我们分享了成果。

### 事实基础

通过采访180多位CIO、CISO、首席技术官（CTO）、首席风险官（CRO）、业务部门主管、监管者、政策制定者、技术供应商，我们获得了生态系统中所有参与者对网络安全整体环境理解的信息。此外，通过对近百个企业技术用户的调查，我们清晰地了解到业务风险、环境威胁及一系列措施的潜在影响。最后，有超过60家世界500强企业参与了针对网络安全风险管理实践的详细调查（见表0-2）。

**表0-2　我们的研究基于大量调查与研究**

| 信息来源 | |
|---|---|
| 采访180多位行业领袖 | CIO、CISO、CTO、CRO及金融服务、保险、医疗保健、高科技及通信、媒体、工业、公共部门等的企业部门主管<br>决策者、监管者、国防及情报界人士<br>地域包含美洲、欧洲、中东及非洲、亚洲 |
| 调查近100个技术管理者 | 内容涵盖：<br>• 最重要的经营风险<br>• 网络攻击风险对业务的影响<br>• 对外部环境的观点<br>• 增强适应力的措施 |
| 针对60多家公司进行网络安全成熟度调查 | 基于180个最佳实践对网络安全风险管理能力进行评估<br>包括金融服务、医疗保健、保险及其他来自美洲、欧洲、中东及非洲和亚洲的参与者 |
| 一系列论坛的验证 | 在有超过500名高管、决策者、学者及意见领袖参加的多个活动中检验：<br>• 在日内瓦、华盛顿、纽约、达沃斯、巴库、布鲁塞尔、大连等地举行的世界经济论坛活动<br>• 麦肯锡召开了由银行业及医疗保健行业CISO参与的论坛 |

### 不同场景与经济影响

我们从被采访人的观点中发现，在未来5～7年网络安全环境如何变化由20多种因素决定，可以概括为威胁的强度及应急响应的质量这两个宏观类别，未来可能出现三种网络安全场景：对网络安全环

境不了解、网络安全环境受到强烈攻击、网络安全环境具有数字适应性。

基于来自采访及调查研究中的信息，我们估计了每个场景将如何影响云计算、移动互联网、物联网等一系列重要科技创新的应用，以及对价值创造的影响程度。

实现数字化适应力的关键措施

在采访及调查研究中，网络安全生态系统中每个参与者已经采取哪些最重要措施，是我们特别关注的，尤为注重公司在自我保护时，在所有业务功能中会采取什么措施。

在定义安全场景、评估经济影响和识别关键措施的时候，我们都会将偶然发现与几十位 CIO、CISO、决策者及其他相关高管一起评审。我们会在硅谷、日内瓦及华盛顿等地的工作会上，麦肯锡组织召开的执行官圆桌会议，大连举行的世界经济论坛新领军者年会上进行这些评审工作。

2014 年 1 月 26 日，我们将自己的研究成果总结发表在一份报告中[3]，并且，在达沃斯世界经济论坛的召开过程中，我们与 80 多位高管及决策者在非公开会议中讨论了我们的研究成果。目前，已有证据表明研究成果逐渐达到了预期目标。《CSO 杂志》解释，我们估计的 3 万亿美元经济影响“吸引了每个人的注意，原因在于，这看上去不仅仅是直接损失，还有因企业和个人回避‘数字化’而未能实现的价值创造值”。[4]

我们展示了研究成果后，麦肯锡及世界经济论坛就开始着手研究要实现数字化适应力需要开展哪些工作。在支持重要机构制定网络安全策略、实施网络安全项目的基础上，麦肯锡进一步帮助企业机构明确应采取的自我保护措施。同时，世界经济论坛举行了数十次有几百家公司参与的工作会议，目的是在网络安全生态系统所有参与者中构建起相互协作支持的关系，达成数字化适应力。

## 注释

[1]不同的组织机构可能使用网络安全、信息安全、IT 安全等词来表达同样的活动，在本书中，我们认为这些说法是可互换的。

[2]World Economic Forum, "Partnering for Cyber Resilience," March 2012.

[3]World Economic Forum, in collaboration with McKinsey & Company, "Risk and Responsibility in a Hyperconnected World," January 2014.

[4]Bragdon, Bob, "When Leadership Gets on Board," *CSO*, June 19th, 2014. www.csoonline.com/article/2365152/security-leadership/when-leadership-gets-on-board.html.

大部分组织机构面临信息资产被盗窃、在线业务流程遭故意破坏等严重的商业风险。如果公司、政府及其他组织机构继续以原有的方式应对这些问题，那么网络攻击的风险会让技术进步的脚步放缓，并在2020年导致高达3万亿美元的经济价值损失。

在更广泛的网络安全生态系统的支持下，为了实现数字化适应力，公司必须让网络安全成为业务及信息技术流程的一部分。

本书主要针对以下三大问题：

（1）网络攻击风险有哪些，在未来几年，其影响将如何演变。

（2）在技术投资和技术创新中，公司如何实现数字化适应力，如何保护自己不受攻击。

（3）企业和公共部门领导该采取怎样的实施步骤来实现数字化适应力目标。

## 3万亿美元处于危险中

公司正面临着网络攻击。有近八成的技术执行官称，与攻击者日益成熟先进的攻击手段相比，他们的防护相对落后。而攻击者的战略战术正在从国家级扩展到不法分子和黑客组织，他们更具破坏性野心。

公司在开展网络安全防护方面可能花费几千万甚至几亿美元的资金，但制定有效的网络安全决策时仍缺少事实根据和有效的流程。在我们详细调查的60多家组织机构中，有1/3的机构网络安全成熟度仅为“初期”，六成仍处于“发展中”，很少达到“成熟”，没有一家是“稳健”的。很多机构只是看上去在这个问题上