Broadview
www.broadview.com.cn

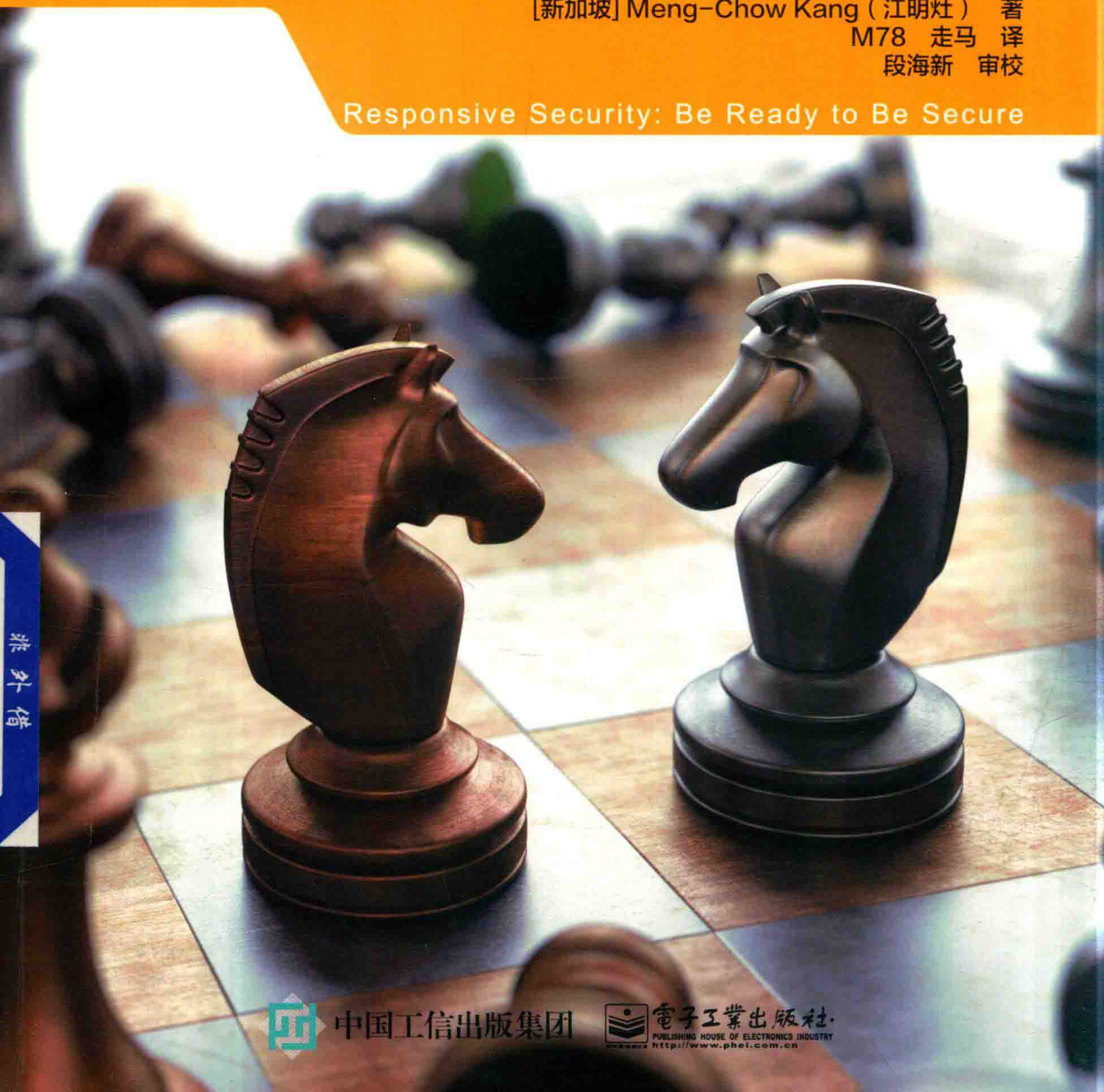
CRC Press
Taylor & Francis Group

响应式安全

构建企业信息安全体系

[新加坡] Meng-Chow Kang（江明灶） 著
M78 走马 译
段海新 审校

Responsive Security: Be Ready to Be Secure



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

Responsive Security: Be Ready to Be Secure

响应式安全

构建企业信息安全体系

[新加坡] Meng-Chow Kang（江明灶） 著
M78 走马 译
段海新 审校

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

图书在版编目（CIP）数据

响应式安全：构建企业信息安全体系 /（新加坡）江明灶（Meng-Chow Kang）著；M78，走马译. —北京：电子工业出版社，2018.4

书名原文：Responsive Security: Be Ready to Be Secure

ISBN 978-7-121-33796-3

Ⅰ. ①响… Ⅱ. ①江… ②M… ③走… Ⅲ. ①企业管理—信息安全—管理体系—研究 Ⅳ. ①F270.7

中国版本图书馆 CIP 数据核字(2018)第 041520 号

策划编辑：刘　皎

责任编辑：郑柳洁

印　　刷：三河市华成印务有限公司

装　　订：三河市华成印务有限公司

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：720×1000　1/16　印张 15.25　字数：244 千字

版　　次：2018 年 4 月第 1 版

印　　次：2018 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）88254888，88258888。

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。

本书咨询联系方式：010-51260888-819，faq@phei.com.cn。

序

这几年，许多组织和安全提供商已经开始转变他们的信息网络安全战略和服务。虽然法律法规和策略合规与否仍是管理层的最高关注因素之一，然而组织的信息安全状况，包括安全弱点，以及针对网络攻击的准备已被视为重点工作。这个安全管理战略转变的趋势是受多方面影响的。其一是这几年媒体报道了导致大量数据泄露和经济损失的多项严重安全事件，并对政府机构和一系列不同行业的国际品牌商业组织产生了恶劣影响。这些事件强化了高层管理者对信息和网络安全的重识，并加强了对组织和个人在这方面的管理。政府和管理机构开始在如何应对网络攻击方面提出相应的要求，受管制的企业必须对这些新的法律法规保持合规。

由于意识到组织内部和外部环境的安全状况信息，特别是与网络系统有关的安全漏洞和最新的攻击手段情报的必须性和重要性，许多安全提供商已把这些安全情报经济化，包装成用户组织可签订的一种信息服务。

安全信息共享也扩展并成熟，到了一个新的阶段，跳出了之前只有安全厂商和安全研究者的经济利益圈子。许多行业已设立了由业内用户组织的安全信息分享和分析架构，并与竞争对手分享安全风险信息。

为提高网络安全应对能力，类似网络靶场（Cyber Range）的技术方案也被商业化，成为安全厂商竞争市场份额的重要项目之一。这种技术提供了一个更真实的训练环境，让组织可以提高安全人员对安全攻击的分析和及时响应的能力。

许多组织的信息安全意识项目也升级到能力训练的层面，不只是安全信息传播。用互动的方法，如防钓鱼邮件的攻击实践练习，能够让用户接触真实钓鱼邮件的样本，从而测试他们的反应是否符合安全实践的要求。

可视度、现状意识、关键对齐、提升应对能力和关注响应能力，这些都是响应式安全的元素。这些元素与近期在业界组织安全管理战略的转变趋势吻合。这是在无计划性和无目的性操纵下的吻合，也可以说是一种巧合。但这个吻合却再次对压电式的信息安全风险管理理论做了一个无计划的验证，表明该理论在技术和商业环境转变下的实用性。

更重要的是，它显示了组织和安全厂商积极地转变网络安全的实践、战略和重点工作，这与提高可视度、应对能力和关注响应能力是吻合的。另外，压电理论也为解释这些战略转变的趋势提供了一个理论基础。

中文版翻译的完成时间超出了我和出版社的计划，我在这期间再次证实了文献中叙述的研究过程、讨论的观点，以及得到的结论，包括其中实现的战略和各种方法是及时的和适用的，而且更适用于当今的信息和网络安全趋势。希望读者能从本书中得到更多信息安全管理的知识和启发，扩展响应式安全的实践，加深在该战略和相关方法上的研究和分享。

致谢

我特别感激 Taylor & Francis 出版社的编辑贺瑞君，电子工业出版社的编辑刘皎与郑柳洁，以及清华大学段海新教授和王永科。

多位信息安全和行动实践研究领域的朋友和同事慷慨无私地与我分享了他们的想法，并在此项工作的各个阶段给出了支持和鼓励，尤其是符传威、Pauline Reich 教授、郑文浩博士及 Bob Dick 教授。我对 CRC 出版社的编辑团队深表感激，尤其是贺瑞君在整个出版过程中给予我的指导、建议和协助。

没有我挚爱的家人毫不动摇的支持、理解和忍耐，本书不可能完成。

谢谢大家。

江明灶（Meng-Chow Kang）

前言

信息安全风险管理是企业和政府机构应对相关信息安全威胁和漏洞的重要组成部分，旨在确保符合管理规定和最佳实践标准，向股东和客户展示自己尽职尽责的工作状态，并以最小成本实现业务目标。

虽然许多研究人员和从业者为信息风险管理的发展和进步做出了一定的贡献，但是现有方法只取得了有限的成功，并且在实践中仍然存在很多问题。尤其是当业务、运营和（或）技术环境面临变化时，这些问题在与信息安全相关的频发事故中是常见的。

信息风险管理所面临的挑战，其本质是复杂性。这种复杂性的出现是由于该领域涉及过多的问题和困境，源于经常互相冲突的要求、需求、认知和影响，包括但不止于人（个人和群体）、过程和技术等，还有问题环境中不同的商业经济发展程度、当局政治期望及文化限制等因素。现有方法只能部分地管理复杂性，还不能很好地满足需求。

为解决遇到的问题和困境，信息安全从业人员必须在实践中反复地反思他们的做法，在过程中不断学习，并且随着其所在风险环境的变化，以迅速的响应和可靠的、演进的方式逐渐提高自己的实践能力。

与此类似，组织需要做好准备，能够随时响应，采取响应式或者压电式（Piezoelectric）的方法，基于组织对响应准备程度的需求应对信息安全风险管理要求，并适应组织所在风险环境不断变化的特性。

响应式方法基于信息风险管理中所谓的“压电理论（Piezoelectric Theory）”的实体理论（Substantive Concept）。压电理论是在实证研究过程中发展出来的，采用了行动实践研究的方法，在六年多的时间内涉及多项案例研究、从业人员采访，并在真实环境中测试了提出的方法。

压电理论指出，如果组织系统中的信息安全实践设计使系统能够重新调整，在系统环境不断变化的风险条件下也能满足系统的整体需求，那么系统环境中新出现的风险状况带来的潜在负面影响将被重新调整所采取的行动措施平衡或消除。

受益于组织系统中的响应行为，环境中突发或新涌现的风险所造成的后果可能会对组织系统产生比较小的负面影响。影响的严重性与安全准备程度和组织的响应能力呈负相关。准备就绪就是指组织能做好准备重新调整其行为，并且能够及时地、系统地采取适当行动来平衡不断变化的风险环境所带来的负面影响。

通过实施和实践，压电理论的响应式方法在解决来自不断变化的风险状况的信息安全需求方面，展现了良好的效果，这些需求都是传统的合规性和面向控制的方法无法有效解决的。

本书回顾了当下认知和实践中存在的问题和困境，介绍了响应式方法的原则和办法，以及安全准备就绪的概念，展示了它在当今信息安全风险环境中的可行性和实用性，鼓励组织更多地采纳并在实践中使用此方法。通过从业人员和研究人员的实践和讨论，我也希望发展并持续响应和调整此方法，解决从业人员面临的不断变化的问题。

目录

1 引言 1

1.1 背景和动机 1
1.2 目的 9
1.3 问题 9
1.4 研究方法 10

2 知识、问题和困境 13

2.1 引言 13
2.2 信息安全 14
2.3 原则和方法 17
2.4 信息安全风险管理战略 43
2.5 信息安全项目 46
2.6 响应变化 58
2.7 当今的信息安全研究和社会学观点 60
2.8 结论 62

3 实践、问题和困境 65

3.1 信息风险管理实践 65
3.2 社会-技术方法 96

4 响应式安全 131

4.1 压电式隐喻 132
4.2 BETA 组织应对新风险和攻击的方法 135
4.3 海啸事件的启示 141
4.4 揭示风险的不确定性并提供风险的能见度 144
4.5 响应、反应及主动性的战略 147
4.6 关键性对齐 150
4.7 在 GAMMA 组织中测试响应式方法 153
4.8 Antinny 蠕虫案例的启示 155
4.9 优化响应式方法 160
4.10 响应式学习 171

5 结论与启示 176

5.1 摘要和结果 176
5.2 对每个研究问题的结论 179
5.3 对理论的启示 183
5.4 对政策和实践的启示 185
5.5 对下一步研究的建议 187

附录 A 行动实践研究周期 189

附录 B 系统探究辩证模型方法 192

附录 C 信息风险管理框架 197

参考资料 203

引言

1.1 背景和动机

信息风险[1]管理的常见目标是确保对信息和信息系统机密性、完整性和可用性的充分保护，这些信息和信息系统对业务顺利进展[2]是关键的和必要的。根据我从事信息安全实践 20 多年的经验，加上不断地与从业人员和研究人员进行交流，我们一致认为对信息风险管理的认识和实践已经落后于其他管理学科，往往不足以支持该领域的从业者需求。

在很大程度上，从业人员的实践活动主要基于个人经验或试错法（trial-and-error），有时还要借用其他知识领域或学科的方法。大多数从业者一直专注于针对已知风险的政策

1 20 世纪末到 21 世纪初，工业界的术语“信息安全”（并非信息安全风险）与“信息风险”之间存在微小的区别。一些组织（包括 ALPHA）开始把它们分成两个职能：前者更关注威胁漏洞和安全解决方案方面的技术；后者更关注通过建立和实现整体框架来管理信息系统和网络中关于人群、方法和技术的威胁、漏洞和解决方案。信息风险管理被这些组织视为一个新的风险管理范例，就像金融机构必须关注和管理的市场风险、结算风险和信用风险一样。本研究中的关注点在后者上——信息风险管理——业界也称为“信息安全风险管理”。

2 信息安全风险管理的目标会根据组织的业务和管理需求的合规性而变化。这一点将在 2.2 节所描述的不同信息安全文献中提到。

合规性（Policy Compliance），即使他们知道每个组织的风险环境是不断变化的，也只在发生安全事故时才进行应对。

对提高我在此领域中实践能力的兴趣驱使我开始研究，以确定或制定一个适用于商业组织中不断变化的风险环境的信息风险管理方案。本书的研究考虑了现有文献资料的知识缺口，以及在实践中观察到的问题和困境。我的思考和分析源于我在此领域的实践经验，这些经验影响了我对问题的研究和得出的结论。我进行的研究已经成为一种用于管理信息安全风险的方法，被称为响应式方法（Responsive Approach），关注组织为应对不断变化的信息风险环境所做的响应准备。

本章介绍了需要研究的信息风险管理中的问题和困境，首先总结实践中的关键问题，然后简单描述响应式安全的调查和研究方法，以后续章节的大纲结尾。

1.1.1 业务、技术和风险发展

我于 2002 年 1 月在 ALPHA[1]开始研究信息风险管理，希望发现或创建一种新方法或增强现有的方法。ALPHA 是一个包括 50 多个国家的跨国金融组织。我是信息风险管理（IRM）[2]小组中的一员，此小组负责亚太地区 11 个城市[3]中 ALPHA 组织的信息风险管理工作。

那个时期，2001 年美国的“9·11”事件[4]和后续的阿富汗战争对全球经济产生了负面影响 (Madrick, 2002; Moniz, 2003)，许多商业组织（包括 ALPHA）基于业务零增长或负增长的前景削减预算，开始采取一系列快速变化的措施以降低成本 (Yourdan, 2002)。

---

1 通用名“ALPHA”，用来代替一家公司的名字，以保持组织匿名。保持研究对象的匿名性是为了保证读者和其他研究人员不会由于其对该组织身份的先验知识而产生先入为主的观念或偏见。

2 在 ALPHA 组织中，IRM 部门的职能是识别和评估信息安全风险，为业务提供缓解、避免、转化方法的应对建议。IRM 的职能也和业务已经采纳的风险应对方法的实现过程跟踪有关，并解决在实现过程中出现的任何问题。

3 曼谷、中国香港、雅加达、吉隆坡、马尼拉、孟买、首尔、新加坡、悉尼、中国台北和东京。大多数信息风险管理活动通常会集中在中国香港、孟买、新加坡、悉尼和东京。

4 要了解更多“9·11”事件的详细解释，请参考“9·11”委员会出版的报告(Kean et al., 2004) (Kean et al. 2004)。

从那以后经济周期似乎每隔几年重演一次。2008 年年底，在我完成研究时，2007 年开始的信贷危机导致的经济衰退现象再次在美国和其他许多国家若隐若现。在 2012 年出版本书英文版时，欧洲爆发经济危机、中国经济增长放缓，亚洲地区的许多国家也有类似现象，美国经济复苏缓慢，这些都表现出经济周期轮回、不稳定和不断变化的迹象。在 2015—2016 年翻译本书时，全球经济仍然没有好转。

由于经济衰退，许多组织（包括 ALPHA）便在外包和离岸[1]上加快推动和执行的速度，以减少与 IT 相关的和许多业务领域的运营开支。向“扩展型企业”演变要求组织增加对外部供应商服务和运营的依赖，并且要创建一个扩展的信任环境，业务部门可以逐渐依靠该信任环境实现目标。这样的改变在业界是常见的 (McDougall, 2002a, 2002b, 2002c)，而且还在继续。监管机构大体上支持此方案，并制定了新政策以使此方案实现全球化 (Bank of Thailand, 2003; Matsushima, 2000; Yakcop, 2000)。虽然这些改变是有计划的，但是许多组织没有做好准备来应对和管理信息安全风险中的相关变化。支持信息风险管理的知识和实践关注的仍然是针对单个组织配置制定内部控制，并且主要依赖合同和服务级别的协议管理外部的风险，但这些风险是内部策略无法充分控制的。

2012 年，随着云计算、虚拟化技术和移动技术的飞速发展，扩展型企业的概念被提升到一个新的水平，首席信息官（CIO）需要利用这些新工具降低运营成本并提高效率。大企业和小企业都逐渐将他们的基础设施、运营平台系统、应用程序和 / 或数据迁移到云数据中心。云数据中心可能由第三方（云服务提供商）提供、自己内部建设，或者两者结合实现。前者通常是首选，可以减少成本支出，同时依靠新的技术服务提高效率。进一步的成本节省也可通过一种共享的架构（称为多租户）实现，而不是为唯一的用户进行设计。在采用这些新兴技术的周期中，我们也看到了类似的困境，其中也存在信息安全和数据隐私的风险和不确定因素，但是新的安全措施的制定，主要还是整合基于以往常用的标准和

1 “离岸”是一个用于表达从相对成熟的站点转移到一个新的站点的术语。“离岸”的目的是利用新站点基础设施和人力资源的低成本优势。这些“离岸”站点通常会设立于发展中国家，如印度、菲律宾和中国。不像外包（与第三方签约），在“离岸”中，经营权仍然属于经营者。

管理要求[1]提出的各种以控制性为主的措施。出于能更快得到经济收益的目的，以及对新风险的无知，大部分不受政府管制的组织[2]也直接引进了这些新的信息技术。

为了获取经济利益和更强的竞争力，2001 年 ALPHA 也像许多其他组织一样，在业务中着手实施了扩展方案，并与其他两个以财务为主的组织合并。这两个合并进来的组织都有和 ALPHA 不同的安全管理制度和看待风险的文化：一个从事投资银行和股票业务，习惯于承受更多的风险；另一个从事投资及资产管理，偏于规避更多的风险。这次合并要求 ALPHA 将具有不同文化、规模、实践、技能和专业、风险承受能力，以及风险管理原则的组织和业务部门整合成一个新商业企业。这也给 IRM 团队的工作带来了新的挑战，它们面临着在保持符合不同实体监管限制和要求的前提下缩小业务之间差距的问题，对新合并的企业也是如此。时至今日，越来越多的合并、收购和合资企业在各种行业中不断涌现，这样做可以获取市场和技术，以提升组织竞争力，并可以缩短从创新到发布新产品之间的转化时间。IRM 团队必须适应持续进行的业务变化，并随其不断改变，以保证发挥应有作用，帮助每一个组织管理其信息安全风险。

随着这些在全球范围内发生的组织机构变化，互联网作为一种企业和个人的通信和协作工具持续增长、扩张 (Furnell, 2002, pp. 1-17; Hall, 2001)，利用软件漏洞的安全事件也随之激增 (AusCERT, 2002)。自此，攻击技术和金融诈骗动机的复杂性也有所增加 (Furnell, 2002, pp. 21-39; Lynley, 2011; Mello Jr., 2013; Skoudis & Zeltser, 2004, pp. 9-13; Whittaker, 2012)。2001 年 9 月，“9・11 事件”发生后不久，一种叫作尼姆达（Nimda）的计算机蠕虫 (CERT/CC, 2001b) 对许多组织的电子邮件、网络和 IT 服务造成了大规模破坏 (Pethia, 2001)。随后，在 2003 年 1 月发生了 SQL Slammer 蠕虫事件 (CERT/CC, 2002b; Krebs, 2003; Microsoft Corporation, 2002)，继而在 2003 年 8 月发生冲击波（Blaster）蠕虫事件

1 例如，云安全联盟（CSA）创建的云控制矩阵（CSA2010），一共包含 99 条高级别控制方案，是安全合规领域用来推荐给安全服务提供商的最佳实践方案。这个计划在计划合规领域间接地为 CCM 达到相关标准合规性的实现计划提供了保证。计划合规领域包括 ISO/IEC 27002、支付卡行业（PCI）、HIPAA、ISACA COBIT 4.1、NIST SP800-53 R3、杰利科论坛和 NERC CIP 出版标准。

2 在一些地区（例如新加坡和香港），监管者把不确定性和不适应性的概念引入行业稳定性描述，例如金融机构等一些管制机构被整顿，促进它们提升技术和服务。

(CERT/CC, 2003b)。同期，来路不明的电子邮件（俗称垃圾邮件[1]）事件也呈指数增长 (The Economist, 2003)。这一切都导致了严重损失[2]，并影响了 ALPHA 的信息安全风险状况。然而，当这些安全事件发生时，信息风险管理者[3]的角色和职责却并不明确，而且许多组织和个人在系统面临破坏时不知如何应对。在互联网上快速浏览 2012 年的重大信息安全相关事件，可以看出在过去的十多年里网络犯罪状况并没有得到改善(Whittaker, 2012)。审视当今组织的信息安全管理可以看出实践方法的改变进展缓慢，但在隧道尽头我们还可以看到一线的光。技术提供商正在设计新的功能，旨在提供更好的预警并检测新的攻击。许多组织正开始部署更多将有助于检测和响应的功能，而不是仅仅着眼于以前普遍使用的预防措施。然而，这也面临更多来自智能移动技术和个人计算设备的挑战，智能手机和平板设备使得雇员和承包人可以更快速地访问企业网络，并可以进出网络转移数据，这是行业内的一种革命性变化，统称为“消费者化的信息技术”(Griffey, 2012; L. L. P. PriceWaterhouseCoopers, 2011)。正如一个信息技术公司在 2009 年宣布的，现在的组织网络是“无边界”的 (Kerravala, 2011)。这样的变化再次给组织和个人带来新的安全和隐私风险问题，困境在于，简单地实施更多的安全规则和控制并不能阻止这些问题发生。

信息安全事件显然是一种计划外的变化，往往源于超出组织控制范围的一系列安全事故。技术进化的影响，以及组织和个人采用某种技术都会引入人们不能预测的风险。为管理这种不断变化的信息风险局面，信息风险管理人员应该如何学习和应对呢？

---

1 关于 SPAM 的定义，没有一致的结论，总体来说，它指的是被不认识的发送者批量发送的未被请求的电子信息，或者发送者预先与接收者没有个人或业务关系。

2 据 Clark 所述 (2003, pp. 40-43)，红色代码（Code Red）病毒造成了 26 亿美元的经济损失；尼姆达蠕虫（Nimda）在 24 小时内影响了全世界范围内的近 250 万服务器和用户；1999 年 3 月，新泽西州的一位程序员释放的梅丽莎（Melissa）病毒造成了至少 8000 万美元的损失。ALPHA 组织也没有逃过这些攻击。

3 IRM 管理者是 IRM 团队的成员之一，其工作是在业务管理中应对风险，执行风险管理任务，例如风险识别和处理，并提供合适的建议和判断，为业务管理层规避识别出的风险。在地区层面，区域信息风险指挥官（RIRO）负责 IRM 的计划和活动；在全球层面（整个 ALPHA 组织内），全球首席信息风险指挥官（CIRO）负责制定全球的策略、战略方向和计划。

1.1.2 常识、标准和实践

信息安全风险管理被普遍认为是识别和评估风险、实施缓解控制[1]并监控这些控制使用的任务，在整个业务系统生命周期内以协调的方式来处理识别出的风险。在安全标准方面，信息安全管理系统（ISMS）的前英国标准 BS 7799 第 2 部分 (BSI, 1999b)，已修订为 ISO/IEC 27001 (2005g, 2013a)，将信息安全风险管理描述为一个“计划-执行-检查-行动”（PDCA）的过程。该标准采用基线控制，如实施 ISO/IEC 27002 (2005i, 2013b) 标准。这种控制也被称为“通用实践”或“最佳实践”，这是一些组织为解决信息风险相关的担忧而普遍采用的安全措施。然而，这些标准中的控制是治标不治本的，并且只是宽泛地进行分类，采用前需要风险管理人员根据风险评估的结果对其进行筛选和优化。这些控制的使用根据个人对风险的理解，主要依赖风险管理人员的知识和经验。同时，国际标准的修订和更新是缓慢的[2]。然而，在不断变化的业务中，在紧缩的预算、缩短的开发时间和快速实现的需求等 IT 环境下，当企业计划为客户提供新服务时，这些只关注已知问题且不能根据变化及时更新的安全控制，将逐渐成为组织内部的障碍。若不实施安全控制的预期收益比实施带来的不确定的或主观的价值高，那么安全控制在实现时往往被忽略、否定或被置于较低优先级。

在信息安全这个领域，我们也一直缺乏标准的信息安全术语，以及实践中对常用词语的解释或术语分类[3]。正如 Jones (2005)指出的，这给信息安全专业带来了诸多不利影响，并伴随较多问题，比如从“组织边缘化问题”、“难以说服组织领导认真采取建议”到“资源利用效率低”等问题。

在新的 IT 系统和网络通信技术领域，企业努力提高生产效率来降低运营和其他开支的成本，或去接触更多的潜在和现有客户以便扩展业务或提供更好的客户服务。即使企业

1 例如 ISO/IEC 27001 (2005g, 2013a)中提到的详细说明。

2 2005 年，国际标准化组织（ISO/IEC JTC 1/SC 27）成功修订了两个标准 ISO/IEC 27001 (2005g)与 ISO/IEC 27002 (2005i)，消除了参与国家关于他们各自主权的标准和控制方案的妥善性和实用性的疑虑（从 2002 年起修订，在此过程中得到了超过 2000 条评论）。2006 年，ISO/IEC JTC 1/SC 27 工作组中的多数项目被重新发起，以修订这些标准并更新以解决新的风险问题。2012 年，该项修订仍然在进行中，一直到 2013 年中旬才成功完成。

3 随着 2700x 系列信息安全管理系统相关标准的制定，这个问题才在 2006 年的 ISO/IEC JTC 1/SC 27 中被关注，包括记录所有相关的词汇和术语的新标准 ISO/IEC 27000。

愿意预先在保护措施方面进行投资，安全标准和最佳实践也难以及时地提供有效的解决方案来应对当前新兴的风险管理需求。一个主要原因是在新技术的领域里，还没有真正的安全技术可以实施，同时，也缺乏可供借鉴的相关系统的安全经验。如果企业希望投资新的方案或方法来解决存在的业务问题或提高业务效率，就会导致企业管理者和 IT 从业者需要承担风险。在大多数情况下，原先为其他业务环境和需求设计的安全措施被重新部署来确保新系统的安全并保护其中的信息。新旧系统之间的差异已经迅速成为安全鸿沟，企业不得不分开管理。组织并不想放弃任何新技术或时机，即使它们可能对其竞争力或赢利能力产生不利影响。近年来，在云计算技术和服务使用方面，正如以上讨论的，我们已经看到了这一幕正在重演。因此，依靠最佳实践方案使企业 IT 技术落后于新进展，具有一定的负面影响。信息风险管理人员应该如何帮助所在组织应对这样一个不断变化的 IT 和业务环境需求呢？

除了应对上述挑战，信息风险管理人员还需要将组织里当前已受管治的信息风险[1]展示给企业管理层，让管理层了解组织的信息安全风险状况。换句话说，信息风险管理人员必须能够衡量 IRM 相关项目活动，以及在安全项目上进行的投资的有效性或能力的表现。在 IRM 团队中，为这种衡量制定合适的指标来获取支持和资源投资是必不可少的。这包括对安全过程进行投资，训练人们具有避开风险和陷阱，以及采取安全措施的意识，定期进行审查和监测来识别安全缺口，以及解决新的安全问题。无论这些行动是否已经全部实现，都不等于能将发生安全事故的概率降为零。组织里执行的信息安全实践和措施必须是可审计的。

在 ALPHA 和其他组织中，包括参与这项研究的组织在内，衡量 IRM 有效性的主要方法是对安全控制的存在及其完整性进行审计和合规性评级，同时包括对安全事故数量和类型进行统计和汇总。这种方法的好处有限，只提供了组织信息风险状况和信息风险管理人员有效性的局部视角，不能提供更全面的意义[2]。

---

1 在本书中信息风险用于表示“信息安全风险”。在这个行业里，这两个词也常被交替使用。

2 2005 年，国际标准化组织（ISO/IEC JTC 1/SC 27）负责制定信息安全相关标准，并开始研究制定国际标准测量信息安全管理的有效性。然而，在度量标准上，来自不同国家实体的标准专家之间存在许多分歧。与此同时，标准专家在测量方法上也没有达成一致。直到 2008 年或之后，也没有一个正式的国际标准出现。这是我参加新加坡标准组织（ISO / IEC JTC 1 / SC 27）的会议所认识到的实际情况。