

大数据时代的网络信息安全及风险评估管理全攻略

信息安全风险管理

从基础到实践

李智勇 张鹏宇 周悦 李伟旗 等 编著

基础篇：明确信息安全风险是如何产生的，该如何进行有效的风险管理

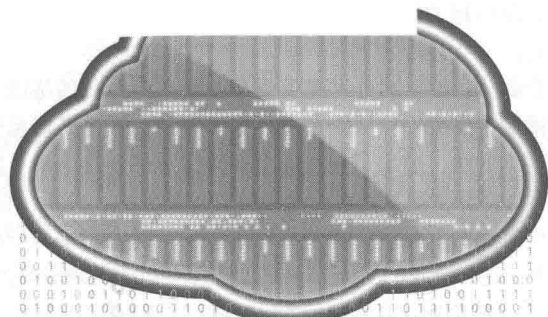
发展篇：基于新的网络安全形势、标准、技术以及应用环境，对信息安全风险管理提出新的思路和方法

实践篇：通过案例实操，更好地掌握信息安全风险识别与分析的方法以及控制措施



化学工业出版社





信息安全风险管理

从基础到实践

李智勇 张鹏宇 周悦 李伟旗 等 编著



化学工业出版社

· 北京 ·

本书以信息安全风险为切入点,站在信息安全风险管理角度阐述网络安全新时代下网络与信息系统安全保障的相关内容,重点提出了信息安全风险识别与分析的方法,明确了信息安全风险控制措施。

全书共分为3个部分:第1部分讲述了信息安全风险管理的基础,明确了信息安全风险定义及构成要素,描述了信息安全风险管理内容及对象,提出了信息安全风险识别分析和信息安全风险处置的基本方法,突出了信息安全风险管理的标准、规范以及信息系统生命周期风险管理的内容;第2部分讲述了信息安全风险管理的发展,分析了信息安全风险形势变化,对信息安全风险产生因素的变化进行描述,对信息安全风险识别与分析的方法进行优化,对信息安全风险控制方法进行优化,对新形势下信息安全风险管理合规性要求的发展进行描述;第3部分重点讲述了信息安全风险管理的实践工作,介绍了风险识别与分析方法有机融合的创新点,对信息安全风险控制的技术措施进行了叙述,列举了风险分析与识别方法以及风险控制方法在税务行业的良好实践,在新型技术应用场景中对信息安全风险识别与分析方法进行了展望。

本书内容实用性强,理论与实践紧密结合,语言通俗易懂,非常适合信息安全技术人员、计算机网络工程师等自学使用,也可用作高等院校相关专业的教材及参考书。

图书在版编目(CIP)数据

信息安全风险管理从基础到实践 / 李智勇等编
著. —北京:化学工业出版社, 2020.2
ISBN 978-7-122-35845-5

I. ①信… II. ①李… III. ①信息安全-风险管理-研究 IV. ①TP309

中国版本图书馆CIP数据核字(2019)第278221号

责任编辑: 栗利娜
责任校对: 刘曦阳

文字编辑: 陈 喆
装帧设计: 王晓宇

出版发行: 化学工业出版社 (北京市东城区青年湖南街13号 邮政编码100011)
印 装: 三河市延风印装有限公司
710mm×1000mm 1/16 印张18½ 字数344千字 2020年6月北京第1版第1次印刷

购书咨询: 010-64518888 售后服务: 010-64518899
网 址: <http://www.cip.com.cn>
凡购买本书, 如有缺损质量问题, 本社销售中心负责调换。

定 价: 69.00元

版权所有 违者必究

近年来,随着网络安全威胁的日益常态化、复杂化和高级化,世界各国都在不断加大对网络空间的部署,尤其是“斯诺登事件”的发生,更使得各国加快了网络安全军事力量建设的步伐。随着信息技术和网络的快速发展,国家安全的边界已经超越地理空间的限制,拓展到信息网络,网络安全成为事关国家安全的重要问题。当前世界主要国家进入网络空间战略集中部署期,国际互联网治理领域出现改革契机,同时网络安全威胁的范围和内容不断扩大和演化,网络安全形势与挑战日益严峻复杂。

新的技术不断涌现,下一代互联网(IPv6)、物联网、三网融合、虚拟化、云计算、大数据等新兴技术在迅猛发展,并且得到越来越多的应用。信息技术带给人类巨大进步的同时,网络与信息系统安全问题所产生的损失、影响也不断加剧,并逐渐成为关系国家安全的重大战略问题,信息系统的安全问题越来越受到人们的普遍关注。信息安全也不单是最初的防毒查毒那么简单的问题,信息安全的中心问题是要保障信息的合法持有和使用者能够在任何需要该信息时获得保密的、没有被非法更改过的“原装的”信息。即通常所说的保密性(confidentiality)、完整性(integrity)和可用性(availability),简称CIA。然而最近,全球权威的信息技术研究及咨询顾问公司Gartner在其最新的研究报告中提出了信息安全的CIA(S)[Safety]模型,打破了传统的三要素,将人员和环境安全加入了其中,即Safety People and Safety Environments。信息安全问题不是单凭技术就可以彻底解决的,它的解决涉及政策法规、管理、标准、技术等方方面面,系统安全问题的解决要站在系统工程的角度来考虑全方位的安全。在这项系统工程中,网络与信息系统安全评测作为检验和评价网络与信息系统安全保护水平的重要方法占有重要的地位,它是信息安全的基础和前提。

随着网络与信息系统规模和复杂性的不断增大,攻击技术和手段不断翻新,网络与信息系统面临的威胁因素越来越多,安全风险防范的难度和复杂性也越来越大。由于资源和能力的限制,不可能消除网络与信息系统中的每一个脆弱点,也不可能防御所有的攻击行为。在信息安全领域,风险控制意味着在成本与效益之间进行权衡,并最终制订相应的安全防御策略,从而有效降低安全风险。以往的信息安全攻防未考虑成本,使得做出的攻防决策并不一定是最优决策。如何在信息安全风险控制和投入之间寻求一种均衡,充分考虑攻防成本有效性问题,利用有限的资源做出最合理的决策,做到“适度安全”,这就给信息安全风险管理工作带来了巨大挑战。准确掌握网络与信息系统的的风险状况,找出风险最大的环节予以防范,避免大规模安全事件的发生,都需要通过信息安全检查、风险

评估和等级保护测评等信息安全风险识别与分析方法来实现，信息安全风险识别与分析在信息安全风险管理中占有重要的地位，发挥了关键作用。

本书以信息安全风险为切入点，站在信息安全风险管理的角度来阐述在网络安全新时代中网络与信息系统安全保障的相关内容，重点提出了信息安全风险识别与分析的方法，明确了信息安全风险控制措施。

本书的核心思想是任何网络与信息系统（虚拟边界或现实边界）的安全风险都是客观存在的，信息安全风险一定是由外部的安全威胁等因素对网络与信息系统自身存在的脆弱性进行有效的作用而产生的，任何安全保障措施都是为了减少自身的脆弱性而更加有效地抵御外部的威胁。本书正是以这个核心思想为指导，从3个部分展开进行阐述的。本书采用了理论与实践相结合的编写原则，其中第1部分注重理论分析，使读者能够明确信息安全风险是如何产生的，该如何进行有效的风险管理；第2部分基于新的网络安全形势、标准、技术以及应用环境，对信息安全风险管理提出新的思路、方法，为更好地实施网络安全防护及关键信息基础设施保护打下牢固的基础；第3部分注重实践展示，通过现实案例与操作使读者能够较好地掌握信息安全风险识别与分析的方法以及信息安全风险控制的流程、方法等。

本书的最大亮点是，提出的理论来自大量实践经验的积累和升华，同时理论又可以指导实际的信息安全风险识别与分析以及风险控制工作。本书的创新点是将现行的信息安全风险识别与分析的方法即等级保护测评、信息安全风险评估和信息安全检查进行有机的融合，可实现一次现场检测、一次数据分析，产生三个层面的检测结果，为下一步进行风险控制提供有力的依据，在第3部分中详细讲述了具体的操作方法和流程。

针对新的网络安全形势，按照新出台的网络安全法律法规和标准制度，基于新型的应用场景，本书提出的信息安全风险识别与分析方法和风险控制措施也在逐步完善与发展。

本书由李智勇、张鹏宇、周悦、李伟旗、王坤提出编写框架、编写思路。其中第1部分（第1章～第5章）由周悦、张鹏宇、邢天柱、蔡忱、张文义、周向明编写；第2部分（第6章～第10章）由张鹏宇、李智勇、李伟旗、邢天柱、蔡忱、王洁编写；第3部分（第11章～第15章）由李智勇、李伟旗、张鹏宇、王洪南、明旭、董庆炳编写。全书由李智勇、张鹏宇、周悦、李伟旗、王坤、邢天柱、蔡忱进行统稿和校对，此外郭欢、郑铁峰、陈磊、邹晔明也参与了本书资料整理等工作。本书在编写的过程中得到了北京软件产品质量检测检验中心（国家应用软件产品质量检测检验中心）和北京中科网威信息技术有限公司的大力支持和帮助，在此一并表示感谢。

由于编者水平有限，书中难免存在不妥之处，恳请各位读者批评指正。

第1部分 信息安全风险管理的基础

- 1.1 信息安全风险含义 / 003
- 1.2 信息安全风险构成 / 005
 - 1.2.1 基本要素 / 005
 - 1.2.2 要素关系 / 006
- 1.3 信息安全风险决定因素 / 007
 - 1.3.1 外部安全威胁 / 007
 - 1.3.2 内部的脆弱性 / 009

- 2.1 信息安全风险管理定义 / 013
- 2.2 信息安全风险管理流程 / 014
- 2.3 信息安全风险管理对象 / 015
 - 2.3.1 物理和环境 / 015
 - 2.3.2 网络和通信 / 016
 - 2.3.3 设备和计算 / 016
 - 2.3.4 应用和数据 / 016
 - 2.3.5 人员和管理 / 017
- 2.4 信息安全风险处置 / 018
 - 2.4.1 风险处置总体描述 / 018
 - 2.4.2 风险处置准备 / 021
 - 2.4.3 风险处置方案制定 / 022
 - 2.4.4 风险处置方案实施 / 024
 - 2.4.5 风险处置效果评价 / 024

第 1 章

信息安全风险产生
003

第 2 章

信息安全风险管理的内容
013

第3章

信息安全风险的识别与分析

027

3.1 信息安全检查 / 027

3.1.1 工作流程 / 027

3.1.2 工作内容 / 027

3.1.3 工作组织 / 029

3.1.4 检查对象选取 / 029

3.1.5 检查工作实施 / 030

3.2 信息安全风险评估 / 033

3.2.1 工作流程及框架 / 034

3.2.2 工作内容 / 037

3.2.3 确定评估对象 / 037

3.2.4 评估工作实施 / 039

3.2.5 风险分析及风险处置 / 045

3.3 信息系统安全等级保护测评 / 047

3.3.1 工作流程 / 047

3.3.2 定级要素及流程 / 047

3.3.3 测评原则及内容 / 048

3.3.4 测评对象 / 049

3.3.5 测评实施 / 050

3.3.6 结果判定 / 052

第4章

信息安全风险的控制

053

4.1 信息安全风险控制的概念 / 053

4.2 信息安全风险处置流程与方法 / 055

4.3 信息安全风险评估有效性检验 / 057

5.1 信息安全风险管理标准规范 / 061

5.1.1 信息安全风险管理国际标准 / 061

5.1.2 信息安全风险管理国内标准 / 068

5.1.3 国内外风险管理标准关系 / 069

5.2 信息系统生命周期的风险管理 / 070

5.2.1 信息系统生命周期的风险评估 / 070

5.2.2 信息系统生命周期的风险管理 / 074

第5章

信息安全风险管理的 合规性要求

061

第2部分 信息安全风险管理的发展变化

6.1 网络安全形势变化 / 081

6.2 信息安全要素变化 / 084

6.3 外部威胁变化 / 084

6.4 内在脆弱性变化 / 086

6.5 安全风险的变化 / 087

第6章

新形势下信息安全风 险的变化

081

第 7 章

新技术应用环境产生的信息安全风险

089

7.1 虚拟化技术平台安全风险 / 089

7.1.1 大数据平台的安全风险 / 089

7.1.2 云计算平台的安全风险 / 092

7.2 移动互联网安全风险 / 102

7.2.1 移动互联网安全威胁 / 102

7.2.2 移动互联网脆弱性 / 105

7.3 工业控制系统安全风险 / 108

7.3.1 工业控制系统安全威胁 / 108

7.3.2 工业控制系统脆弱性 / 110

7.4 信息安全保障能力的不足 / 112

第 8 章

新形势下信息安全风险识别与分析方法的优化

115

8.1 现行方法存在的局限性 / 115

8.2 现行方法融合的必要性 / 117

8.3 现行方法融合的基本思路 / 119

8.4 现行方法融合的主要内容 / 121

8.4.1 检测目标统一定义 / 121

8.4.2 信息资产统一定义 / 122

8.4.3 外部威胁统一定义 / 122

8.4.4 内在脆弱性统一定义 / 123

8.4.5 风险分析统一定义 / 125

8.5 新型风险识别与分析方法的提出 / 128

8.6 新型风险识别与分析方法的优化 / 128

8.6.1 工作原理的优化 / 128

8.6.2 工作流程的优化 / 129

8.6.3 工作内容的优化 / 132

第9章

新形势下信息安全风险控制的方法优化

135

9.1 关键信息基础设施安全保护 / 135

9.1.1 明确关键信息基础设施保护

对象 / 135

9.1.2 我国关键信息基础设施面临的

威胁 / 136

9.1.3 制定关键信息基础设施安全保护标准

规范 / 137

9.1.4 网络安全等级保护与关键信息基础

设施保护 / 138

9.2 网络安全态势感知 / 138

9.2.1 网络安全态势感知概念 / 138

9.2.2 网络安全态势感知的内容 / 139

9.2.3 网络安全态势感知的方式优化 / 140

9.3 虚拟化应用安全保护 / 141

9.4 威胁情报分析 / 141

9.5 构建纵深网络安全防御体系 / 144

9.6 新技术应用环境下的信息安全风险

控制 / 146

9.6.1 虚拟化平台风险控制 / 146

9.6.2 物联网风险控制 / 147

9.6.3 移动互联网风险控制 / 148

9.6.4 工业控制系统风险控制 / 149

第 10 章

新形势下信息安全风险管理合规性要求的发展

151

10.1 新形势下信息安全风险管理标准体系 / 151

10.2 网络安全法 / 153

10.2.1 网络安全法立法的背景 / 153

10.2.2 网络安全法的基本内容 / 154

10.2.3 网络安全法的作用及意义 / 155

10.3 关键信息基础设施安全保护条例 / 155

10.3.1 安全保护条例主要内容 / 155

10.3.2 安全保护条例的局限性 / 157

10.3.3 安全保护条例与网络安全等级保护关系 / 158

10.4 网络安全等级保护相关标准 / 158

10.4.1 现有等级保护政策和标准体系 / 158

10.4.2 网络安全等级保护制度 2.0 / 159

10.5 网络产品和服务安全审查办法 / 162

10.5.1 安全审查办法主要内容 / 162

10.5.2 安全审查办法出台后的影响 / 163

10.5.3 安全审查办法意义及作用 / 163

第3部分 信息安全风险管理的实践

- 11.1 基本原理 / 167
- 11.2 流程方法 / 168
 - 11.2.1 工作流程 / 168
 - 11.2.2 工作方法 / 177
- 11.3 实施组织 / 178
- 11.4 对象确定 / 179
- 11.5 准备阶段工作 / 183
- 11.6 实施阶段工作 / 184
 - 11.6.1 现场培训 / 184
 - 11.6.2 资产识别 / 185
 - 11.6.3 威胁识别 / 186
 - 11.6.4 技术安全检测 / 188
 - 11.6.5 管理安全检测 / 191
 - 11.6.6 渗透测试 / 193
 - 11.6.7 已有安全措施分析 / 196
 - 11.6.8 脆弱性分析与赋值 / 196
 - 11.6.9 现场工作小结 / 196
- 11.7 总结阶段工作 / 197
 - 11.7.1 数据整理 / 197
 - 11.7.2 综合分析 / 199
 - 11.7.3 报告编制 / 200

第 11 章

风险识别与分析方法
融合——信息安全风
险测评

167

第 12 章

信息安全风险控制方法——安全基线配置 203

- 12.1 明确安全基线配置作业需求 / 203
- 12.2 建立安全基线配置管理规范 / 204
- 12.3 制定安全基线配置模板 / 205
- 12.4 现场基线配置检查确认 / 208
 - 12.4.1 技术基线检查 / 209
 - 12.4.2 管理基线审核 / 212
- 12.5 基于安全基线要求的整改加固 / 213
- 12.6 安全基线配置模板的修订 / 215

第 13 章

信息安全风险控制方法——服务器信息安全加固 217

- 13.1 信息安全加固的目的及意义 / 217
 - 13.1.1 精准实施信息安全风险控制 / 217
 - 13.1.2 紧密结合等级保护整改建设 / 218
 - 13.1.3 严格依据等级保护测评结果 / 218
 - 13.1.4 有效提高等级保护测评符合率 / 218
- 13.2 信息安全加固的重点及难点 / 220
 - 13.2.1 安全加固可行性分析 / 220
 - 13.2.2 安全加固工作重点 / 221
 - 13.2.3 安全加固工作难点 / 222
- 13.3 信息安全加固原则及范围 / 223
 - 13.3.1 安全加固的原则 / 223
 - 13.3.2 安全加固的范围 / 223
- 13.4 信息安全加固流程及组织 / 224
 - 13.4.1 安全加固流程与方法 / 224
 - 13.4.2 安全加固的组织 / 226

13.5 信息安全加固实施内容 / 229

13.5.1 准备阶段内容 / 229

13.5.2 实施阶段内容 / 231

13.5.3 分析总结阶段内容 / 238

13.5.4 操作实例 / 239

14.1 税务系统信息安全风险测评实践 工作 / 241

14.2 税务系统信息安全基线配置实践 工作 / 243

14.2.1 计划准备环节 / 243

14.2.2 现场实施环节 / 243

14.2.3 成果输出环节 / 244

14.3 税务系统服务器信息安全加固实践 工作 / 244

15.1 移动互联网环境的风险测评 / 247

15.1.1 移动智能终端安全风险测评 / 247

15.1.2 移动传输网络安全风险测评 / 248

15.1.3 移动应用安全风险测评 / 249

15.2 虚拟化环境的风险测评 / 250

15.2.1 虚拟化环境安全风险分析 / 250

15.2.2 虚拟化环境安全风险测评 / 251

15.3 工业控制系统的风险测评 / 252

15.3.1 工业控制系统测评原则 / 252

第 14 章

信息安全风险管理的
良好实践

241

第 15 章

风险识别与分析方
法在新技术环境中
的应用

247

附录

257

- 15.3.2 工业控制系统测评流程 / 253
- 15.3.3 工业控制系统测评工具 / 254

- 附录1 信息安全风险测评表单 / 257
- 附录2 网络与信息系统安全基线配置
表单 / 267
- 附录3 服务器信息安全加固表单 / 274

参考文献 / 280

第 1 部分

信息安全风险管理的基础



第1部分主要讲述了信息安全风险管理的基础内容，首先对信息安全风险组成、信息安全风险产生原因进行了描述，对信息安全风险管理的对象及内容进行了叙述，明确了信息安全风险处置的基本方法；列举了信息安全风险管理标准，对信息系统生命周期风险管理进行了描述；对信息安全风险识别与分析的三类主要方法进行了较为详细的叙述，并提出了信息安全风险控制的基本思路与方法。