第一图书网, tushu007.com

<<信息安全保卫战>>

图书基本信息

书名：<<信息安全保卫战>>

13位ISBN编号：9787302309154

10位ISBN编号：7302309159

出版时间：2013-1

出版时间：清华大学出版社

作者：雷万云

页数：259

字数：372000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

前言

社会信息化，已成不可阻挡的历史潮流，成为大趋势，引发可怕的信息安全威胁。
可以看到，随着新一代信息技术的飞速发展和应用，给我们带来好处的同时，也相应地给我们带了前所未有的信息安全威胁。
信息安全逐渐告别传统的病毒感染、网站被黑及资源滥用等时代，迈进了一个复杂多元、综合交互的新时期。
如何在有效利用信息技术的同时，积极应对和及时识别和规避这些风险，形成新的信息安全建设策略与实践，打好信息安全保卫战，是我们大家必须面对的主题，也是本书讨论和论述的话题。
《信息安全保卫战》是笔者有关企业信息化建设系列丛书之一，她的出版和近年来笔者在清华大学出版社出版的《云计算——企业信息化建设策略与实践》、《云计算——技术、平台及应用案例》以及《信息化与信息管理实践之道》构成一个完整的企业信息化建设四部曲。
第一本云计算是云计算的普及图书，全面系统地论述了云计算的概念、技术以及市场发展状况，并在此基础上进一步阐述基于云计算的企业信息化建设策略与实践。
第二本云计算是在第一本基础上深入阐述云计算的概念、技术和架构以及国内外的应用案例。
第三本是有关企业信息化与信息管理的实战图书，从信息化规划、管控、标准和项目实施等层面论述企业信息化建设的策略、方法与实践。
第四本也就是本书是对信息安全这一主题的全面深入论述。
本书基于云计算理念，提出一个组织的整体安全概念，从组织的战略、业务出发，结合安全标准和业界最佳实践，形成系统的方法路径，帮助组织定位安全现状，了解安全需求，实施安全建设，以打赢我们的信息安全保卫战。
目前业界已有众多的信息安全书籍，但大都是针对某一系统的信息安全具体的技术探讨。
本书旨在对一个组织信息安全建设提供一个集成的、标准的信息安全框架，为组织信息安全平台的建设、设计、实施提供指导。
全书为11章，其主要内容如下。
第1章首先从全球一体化、信息技术的发展利用等方面综述了信息化社会的信息安全威胁，并进一步阐述了企业信息化的发展应用对企业信息安全带来的威胁。
第2章通过企业合规经营风险分析引入企业风险与信息安全的关系，说明信息安全是确保企业合规经营的基本保障。
第3章在分析企业信息安全现状的基础上进一步论述了企业信息安全建设的目的意义，说明打赢信息安全保卫战的重要性。
第4章介绍了信息安全发展历程和国内外信息安全标准。
第5章在分析云计算安全问题基础上进一步提出了云计算安全框架，并论述了云计算安全标准的发展情况，最后进一步综述了国内外先进的云计算安全提供商的云计算安全解决方案。
第6章引入企业信息安全框架概念，并全面、完整地阐述了企业信息安全框架的定义、内容以及建设意义。
第7、8、9章分别对信息安全框架的三个组成部分：信息安全管理、运维和技术体系深入介绍和描述。
第10章从一个组织的战略出发来全面考虑组织的信息安全的规划、管理、技术、运维等完整的信息安全框架设计与实施的策略与方法并进行了系统论述，给出一个信息安全框架建设的方法和路径，第11章并给出了相应的实践案例。
本书定位于一个组织（包括政府、区域和城市、企业等）信息安全建设理论、技术、策略方法以及实践案例介绍和论述，从系统工程层面来论述，体现企业信息安全建设的方法论。
本书主要面向企业的CEO和企业管理人员，企业的CIO和从事信息化、信息安全建设的IT人；其次是咨询公司的业务和IT咨询人员以及企业信息安全项目实施人员；当然对于政府的管理人员来讲，是一个很好的信息安全知识水平和工作思路的提升学习的最佳参考书；对于大专院校的师生们进一步系统地认识企业信息安全建设、企业IT的实际情况，企业和社会信息安全建设思路是一个绝好的参考书；最后，对于从事企业信息安全的服务提供商也是一个很好的值得借鉴的参考书，因为只有深刻了解企

业的需求、信息安全建设的系统思维，才能实施好企业信息安全项目。
本书由雷万云博士主持编写，华为技术公司、启明星辰信息安全公司和深信服科技公司相关专家参加了编写。
他们分别是：华为企业网安全首席技术官何利文，IEEE高级会员，全国青联IT联谊会常务理事，英国谢菲尔德大学博士，曾任英国电信首席安全研究员；华为数据中心安全高级营销顾问时成阁；华为企业网安全高级营销顾问黄菲一。
启明星辰信息安全高级咨询顾问刘德文和张艳博士。
深信服科技市场技术总监殷浩先生。
雷万云博士撰写了大纲和各章节的主要内容要点，对全书各章节内容进行了优化、统稿和对全部内容进行了审阅，并撰写了前言。
其中第1章、第3章和第4章由雷万云博士撰写；第2章由雷万云博士、王静撰写；第5章由雷万云博士、何利文、黄菲一撰写；第6章由雷万云博士、刘德文、张艳博士撰写；第7章由刘德文、雷万云博士、张艳撰写；第8章由何利文、时成阁、刘德文、雷万云博士撰写；第9章由何利文、时成阁、雷万云博士、殷浩撰写；第10章由雷万云博士、刘德文、张艳编写，第11章由雷万云博士、刘德文、张艳、殷浩编写。
李懿凌和韩金利画了书中的大部分示图。
由于作者水平有限，书中难免有疏漏和不当之处，敬请读者批评指正。
最后，谨向帮助、支持和鼓励我完成本书的我的家人、同事、领导、朋友、合作伙伴以及清华出版社的领导、编辑表示真挚的感谢！
博士2012年国庆假期于北京

内容概要

本书定位于一个组织信息安全建设理论、技术、策略方法以及实践案例的介绍和论述，描述当今信息化社会环境下，如何打赢信息安全保卫战。
全书分为11章，首先综述了信息化社会的信息安全威胁，说明打赢信息安全保卫战的重要意义。
其次论述了信息安全发展历程和信息安全标准以及云计算安全发展状况。
再次，提出了企业信息安全框架的概念和内容，最后给出了一个组织信息安全框架建设的策略与方法以及实践案例，帮助读者形成信息安全建设的思路和系统的方法路径以及最佳实践。

本书面向组织的管理者、CIO和从事信息化、信息安全建设的IT人；其次是咨询公司的业务和IT咨询人员以及企业信息安全项目实施人员。
对于大专院校的师生们进一步系统地认识企业信息安全建设、形成科学系统的信息安全建设思路是一个绝好的参考书。

基于云计算理念，本书提出一个组织的整体安全框架，从组织的战略、业务出发，结合安全标准和业界最佳实践，形成系统的信息安全建设方法路径。

帮助组织定位安全现状，了解安全需求，实施安全建设，以打赢信息安全保卫战。

作者简介

雷万云先生先后从中国电子科技大学、西安交通大学、西北工业大学毕业，分别获得电子信息科学技术专业的学士、硕士和博士学位，并在德国技术物理研究院学习工作二年。

雷博士曾任国家某大型国防科技研究所副所长、国家电子信息技术领域技术专家、国家电子信息技术学报编委会主任、主编，某大型金融证券资讯公司总裁。
雷博士有20余年信息化方面的研究开发、实施和管理经验，是管理与信息化方面的专家；国家认证的高级企业信息管理师，尤其对集团企业和医药行业的信息化建设有深刻理解和最佳实践。
近年来致力于云计算系统研究，并著有《云计算——企业信息化建设策略与实践》和《云计算——技术、平台与应用案例》两本书，现从事医药行业信息化管理工作。

书籍目录

第1章 信息化社会的信息安全威胁
1.1 信息化是世界发展的大趋势
1.1.1 社会信息化的趋势
1.1.2 新IT技术应用带来新风险
1.2 全球一体化的趋势
1.3 企业发展与竞争的趋势
1.4 信息安全威胁综述
1.4.1 信息安全面临的主要威胁
1.4.2 信息安全问题分析
1.4.3 信息安全管理现状分析
1.4.4 信息安全形势和事故分析
1.4.5 信息安全对企业威胁分析
第2章 企业风险与信息安全
2.1 企业合规风险
2.1.1 从企业合规风险看IT管理风险
2.1.2 从SOX合规性看我国IT内控规范
2.1.3 安全合规性管理
2.2 企业数据泄密风险
2.2.1 数据安全评估
2.2.2 数据安全风险分析
2.2.3 数据安全风险治理
2.3 从企业风险分析认识信息安全风险
第3章 信息安全管理内涵
3.1 信息安全概述
3.1.1 传统信息安全的定义
3.1.2 信息安全技术与信息安全管理
3.1.3 当代信息安全的新内容
3.1.4 信息安全框架及其实施内涵
3.2 信息安全建设阶段分析
3.3 信息安全建设目的意义
第4章 信息安全发展与相关标准
4.1 信息安全发展
4.1.1 信息安全发展历程
4.1.2 信息安全发展趋势
4.2 信息安全管理标准的提出与发展
4.3 ISO/IEC 2700X系列国际标准
4.3.1 信息安全管理体系（ISO/IEC 27001: 2005）
4.3.2 信息安全管理实施细则（ISO/IEC 27002）
4.4 信息安全管理实施建议与指导类标准
4.5 信息安全测评标准
4.5.1 美国可信计算机安全评估标准（TCSEC）
4.5.2 国际通用准则（CC）
4.6 信息安全国家标准简介
4.7 国家信息安全等级保护体系
4.7.1 国家信息安全保障工作的主要内容

4.7.2 开展等级保护工作依据的政策和标准
4.7.3 等级保护工作的具体内容和要求
4.7.4 中央企业开展等级保护工作要求
第5章 云计算安全
5.1 云计算安全问题分析
5.1.1 云计算的主要安全威胁分析
5.1.2 从云计算服务模式看安全
5.2 云计算安全框架
5.2.1 架构即服务（IaaS）
5.2.2 网络即服务（NaaS）
5.2.3 平台即服务（PaaS）
5.2.4 数据即服务（DaaS）
5.2.5 软件即服务（SaaS）
5.2.6 安全是一个过程
5.3 云计算安全标准化现状
5.3.1 国际和国外标准化组织
5.3.2 国内标准化组织
5.4 云计算安全解决方案概述
5.4.1 亚马逊云计算安全解决方案
5.4.2 IBM虚拟化安全sHype解决方案
5.4.3 IBM基于XEN的可信虚拟域（TVD）
5.4.4 VMware虚拟化安全VMSafe
5.4.5 Cisco云数据中心安全解决方案
5.4.6 华为云安全解决方案
5.5 云计算安全开放命题
第6章 企业信息安全框架
第7章 信息安全管理体系
第8章 信息安全运维体系
第9章 信息安全技术体系
第10章 信息安全体系建设
第11章 信息安全建设案例
参考文献

章节摘录

版权页： 插图： 2.组织机构与职责分工 成立由企业主管领导任责任人的信息安全管理机构，管理机构具有以下职责：（1）组织、协调和指导本企业信息化建设、使用和维护开发工作；（2）组织制定信息化安全策略、流程和各种规章制度；（3）组织信息安全风险评估及信息安全教育培训；（4）组织信息化设备、设施、介质等授权使用和管理、维护、监督检查；（5）落实年度安全计划、报告等；（6）与国家相关主管部门建立日常工作关系；（7）执行国家相关法律法规。
3.企业信息安全制度建立 企业信息安全管理机构组织建立相应的信息安全管理制度，明确岗位职责，实行领导责任制，层层落实，责任到人，使各个环节的每个工作人员明确应承担的职责和义务。
信息安全管理制度要涵盖信息化的产生、存储、处理、传输、归档和销毁的全过程，从人员、物理设施与环境、设备与介质、运行与开发和数据安全等诸多方面制定相应的制度。
4.信息安全管理文件体系建立 （1）确立信息安全管理体系范围和体系环境所需的过程；（2）战略性和组织化的信息安全管理环境：（3）组织的信息安全风险管理方法；（4）信息安全风险评价标准以及所要求的保证程度；（5）信息资产识别的范围。
信息安全文件体系也可能在其他信息安全管理体系的控制范围内。
在这种情况下，上下级控制的关系有下列两种可能：下级信息安全管理体系不使用上级信息安全管理体系的控制：在这种情况下，上级信息安全管理体系的控制不影响下级信息安全管理活动。
下级信息安全管理体系使用上级信息安全管理体系的控制：在这种情况下，上级信息安全管理体系的控制可以被认为是下级信息安全管理体系策划活动的“外部控制”。
尽管此类外部控制并不影响下级信息安全管理体系的实施、检查、措施活动，但是下级信息安全管理体系仍然有责任确认这些外部控制提供了充分的保护。
5.信息安全管理过程建立 （1）IT规划管理：信息化规划制定和跟踪的流程。
（2）IT制度管理：信息化管理制度体系化建设和完善的流程。
（3）IT资源管理：对IT资源（包括人员、财务和IT资产）申请、审核、配备、评估的流程。
（4）监督管理：依据IT规划和制度对IT管理工作进行监督、检查和跟踪整改的流程。
（5）违规管理：对IT管理制度执行过程中的违规行为进行纠正与处罚的流程。
（6）外部环境：对影响IT管理目标实现的外部因素进行跟踪、响应、控制的流程。
外部环境包括供应商管理、市场、经济环境、金融安全等。

编辑推荐

《信息安全保卫战:企业信息安全建设策略与实践》基于云计算理念，提出一个组织的整体安全框架，从组织的战略、业务出发，结合安全标准和业界最佳实践，形成系统的信息安全建设方法路径。
《信息安全保卫战:企业信息安全建设策略与实践》帮助组织定位安全现状，了解安全需求，实施安全建设，以打赢信息安全保卫战。

第一图书网, tushu007.com

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com