高等学校计算机类国家级特色专业系列规划教材

信息安全管理与工程

王春东 主编
杨宏 莫秀良 岳丽 副主编

清华大学出版社

高等学校计算机类国家级特色专业系列规划教材

信息安全管理与工程

王春东 主编
杨宏 莫秀良 岳丽 副主编

清华大学出版社
北京

内 容 简 介

本书以目前信息系统安全管理与工程存在的问题和发展要求为写作方向，以编者所在一线教师团队多年来相关教学以及研究工作为基础，系统阐述了信息安全管理与工程的体系结构、基本框架、法律规范等相关知识。全书共分为10章，各章内容既相互独立，又相互联系。第1章是信息安全管理体系；第2章详细介绍信息安全风险管理；第3章是基本信息安全管理；第4章是重要信息安全管理措施；第5章是信息安全管理华为典型实例；第6章是信息安全工程原理；第7章是信息安全工程实践；第8章是信息安全保障；第9章介绍信息安全标准；第10章详细阐述信息安全法律政策和道德规范。

本书可供信息安全、计算机科学与技术专业的本科学生，以及相关领域的研究人员、教师、研究生和工程技术人员参考。

图书在版编目(CIP)数据

信息安全管理与工程/王春东主编. —北京：清华大学出版社，2016
高等学校计算机类国家级特色专业系列规划教材
ISBN 978-7-302-41636-4

Ⅰ. ①信… Ⅱ. ①王… Ⅲ. ①信息安全—安全管理—高等学校—教材 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2015)第228400号

责任编辑：汪汉友　赵晓宁
封面设计：傅瑞学
责任校对：李建庄
责任印制：刘海龙

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954

印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：14.75　　**字　　数**：367千字
版　　次：2016年6月第1版　　**印　　次**：2016年6月第1次印刷
印　　数：1～2000
定　　价：34.50元

产品编号：065799-01

前　言

随着信息化和网络化的发展，信息安全问题日益突出。“信息安全管理与工程”成为国内许多高校信息安全专业、计算机科学与技术专业的必备课程。目前国内关于信息安全管理及信息安全工程的书籍特别多，但这些书籍更多偏重于理论知识。本书理论联系实际，引用了业界典型信息安全管理案例，使内容更加充实。书中多处运用图形和表格来解释难懂的概念，图文并茂，易懂易学，非常适合不同水平的读者阅读。本书是作者及教学团队十余年来在信息安全管理与工程方面所做工作的总结。希望本书的出版，能为我国信息安全专业的发展、学科的建设和创新突破带来一些启迪和帮助。

由于作者水平有限，本书遗漏和不妥之处在所难免，恳请读者批评指正。

编　者

2016 年 4 月

目　录

第 1 章　信息安全管理体系

导入语：本章系统地介绍了信息安全管理体系方面的内容，包括信息安全管理的基本概念和信息安全管理体系建设。信息安全管理的基本概念部分，介绍了信息安全管理的作用、风险管理的概念和作用、安全管理控制措施的概念和作用。信息安全管理体系建设部分，介绍了过程方法与 PDCA 循环，以及建立、运行、评审与改进 ISMS。

本章主要知识结构如图 1.1 所示。

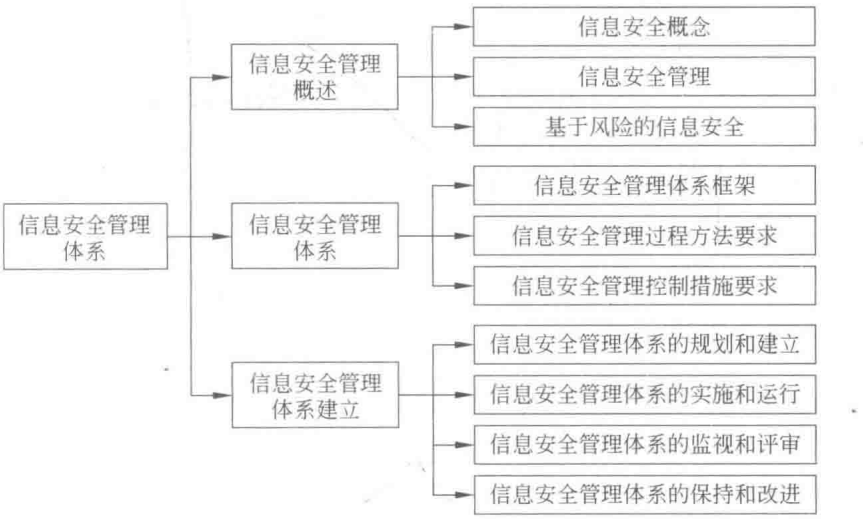

图 1.1　本章主要知识结构框图

考核目标：理解信息安全“技管并重”原则的意义与成功实施信息安全管理工作的关键因素。理解信息安全风险的概念，包括资产价值、威胁、脆弱性、防护措施、影响、可能性。理解风险评估是信息安全管理工作的基础。理解风险处置是信息安全管理工作的核心。理解安全管理控制措施是管理风险的具体手段。了解 11 个基本安全管理控制措施的基本内容。

1.1　信息安全管理概述

随着全球网络的持续发展，网际互联对于通信系统和计算系统的流畅运作变得愈发重要。然而，日益增多的病毒、蠕虫攻击事件以及黑客网络犯罪表明：当前的信息技术还存在诸多缺陷，因而有必要提高信息系统的安全。

信息安全管理是通过维护信息的保密性、完整性和可用性等来管理和保护信息资源的一项体制，是对信息安全保障进行指导、规范和管理的一系列活动和过程。

1.1.1　信息安全概念

客观世界是由物质、能量和信息三要素构成。现在人类社会进入了一个崭新的电子信

息化时代，信息安全变得越来越重要。

信息是一种资产，像其他重要的业务资产一样，它对组织具有价值，因此需要妥善保护。信息安全的含义是通过各种计算机、网络和密钥技术，保证在各种系统和网络中传输、交换和存储的信息的机密性、完整性和真实性。信息安全的结构层次分为物理安全、安全控制和安全服务。为了更好地理解信息安全管理，必须熟悉一个组织机构有价值的关键信息的特性。

(1) 保密性。为了确保只有那些被授予特定权限的人才能够访问到信息，信息的保密性依据信息被允许访问对象的多少而不同。根据信息的重要程度和保密要求将信息分为不同密级，所有人员都可以访问的信息为公开信息，需要限制访问的信息为敏感信息或秘密信息。

(2) 完整性。保证信息和处理方法的正确性和完整性。信息完整性一方面指在使用、传输、存储信息的过程中不发生篡改信息、丢失信息、错误信息等现象；另一方面指信息处理方法的正确性，执行不正当的操作，有可能造成重要文件的丢失，甚至整个系统的瘫痪。

(3) 可用性。确保那些已被授权的用户在他们需要的时候，可以访问到所需信息，即信息及相关的信息资产在授权人需要的时候，可以立即获得。例如，通信线路中断故障、网络的拥堵等会造成信息在一段时间内不可用，影响正常的业务运营，这是信息可用性的破坏。提供信息的系统必须能适当地承受攻击并在被攻击后得到恢复。

1.1.2 信息安全管理

一个成功的信息安全项目，要将上述的各种概念结合起来，以减少信息资产的风险，必须通过细致的管理来实现。站在较高的层次上看信息和网络安全的全貌就会发现，安全问题实际上都是人的问题，单凭技术无法保证整个系统的安全。

信息安全管理的定义：组织中为了完成信息安全目标，针对信息系统，遵循安全策略，按照规定的程序，运用恰当的方法，而进行的规划、组织、指导、协调和控制等活动。

信息安全管理的目标如下：防止未授权存取；防止未被授权的人进入系统；用户意识、良好的口令管理、登录活动记录和报告、用户和网络活动的周期检查等都是防止未授权存取的关键；防止泄密，防止已授权和未授权的用户相互存取重要信息，这也是计算机安全的一个重要问题；防止用户拒绝系统的管理，这应由操作系统来完成，一个系统不应被一个有意试图使用过多资源的用户损害；防止丢失系统的完整性，这与系统管理员的实际工作和保持可靠的操作系统有关。

信息安全是一个多层面、多因素的过程。如果组织凭着一时的需要，想当然去制定一些控制措施和引入某些技术产品，都难免存在挂一漏万、顾此失彼的问题，使得信息安全这只“木桶”出现若干“短板”，从而无法提高信息安全水平。正确的做法是参考国内外相关信息安全标准与最佳实践过程，根据组织对信息安全的各个层面的实际需求，在风险分析的基础上引入恰当控制，建立合理安全管理体系，从而保证组织赖以生存的信息资产的保密性、完整性和可用性。

信息安全管理是通过维护信息的保密性、完整性和可用性，来管理和保护组织所有的信息资产的一项体制；是组织中用于指导和管理各种控制信息安全风险的一组相互协调的活动，有效的信息安全管理要尽量做到在有限的成本下，保证安全风险控制在可接受的范围。

1.1.3 基于风险的信息安全

安全管理是信息安全中非常重要的一环，要实现较完善的安全管理，必须分析、评估安全需求，建立满足需求的计划，实施这些计划，并进行日常维护和管理。由此可见，安全管理过程的第一步就是要建立一个全局安全目标，然后将其整合到机构的安全政策中去。实现这一要求的关键是对风险的评估，将风险减少到可以接受的水平。

1. 风险评估概述

识别了机构的威胁和漏洞后，就可以评估每个漏洞的相关风险了。这是通过风险评估过程来完成的。风险评估给每项信息资产分配一个风险等级或者分数。此数字可用于评估每项易受攻击的信息资产的相关风险，并在风险控制过程中促进比较等级的发展。

风险＝出现漏洞的可能性×信息资产的价值－当前控制减轻的风险概率
＋对漏洞了解的不确定性

其中，“出现漏洞的可能性”是指成功攻击机构内某个漏洞的概率。在风险评估中，要给成功攻击漏洞的可能性指定一个数值。国家标准与技术协会在 Special Publication 800-30 中推荐，这个可能性应指定为 0.1～1.0 之间的一个值。比如，在室内被陨石击中的可能性是 0.1。明年收到至少一封带病毒或蠕虫的电子邮件的可能性是 1.0。还可以选择使用 1～100 中的数字，但不能使用 0，因为可能性为 0 的漏洞已从资产/漏洞列表中删除。

2. 信息安全风险评估原则

1）自主

自主指组织机构内部的人员管理和指导组织机构的信息安全风险评估。这些人负责指导风险管理活动，并对组织机构的安全工作做出决策。这种方法使评估能够考虑组织机构的与众不同的情形和环境。自主要求：通过领导信息安全风险评估并对评估过程进行管理，负责信息的安全。最终对组织机构的安全工作做出决策，包括实现哪些改进和采取哪些行动。

2）适应度量

一个灵活的评估过程可以适应不断变化的技术和进展，既不会受限于当前威胁源的严格模型，也不会受限于当前公认的“最佳”实践。因为信息安全和信息技术领域变革非常迅速，所以需要一个适应性强的度量集，组织机构及其独特的环境可以据此进行评估。适应度量要求：定义公认的安全实践、已知的威胁源和技术缺陷目录；能适应信息目录变化的评估过程。

3）已定义过程

已定义的过程描述了信息安全评估程序依赖于已定义的标准化评估规程的需要。使用一个已定义的评估过程有助于过程的制度化，保证评估的应用能达到一定程度的一致性。一个已定义的过程要求：为执行评估分配责任；定义所有的评估活动；规定评估过程所需的所有工具、工作表和信息目录；为记录评估结果创建通用的格式。

4）连续过程的基础

组织机构必须实施基于实践的安全策略和计划，以便逐渐改进自身的安全状态。通过实施这些基于实践的解决方案，组织机构就能够开始将最佳的安全实践制度化，使其成为组织机构日常开展业务方法的一部分。安全改进是一个连续的过程，信息安全风险评估的结

果为连续的改进奠定了基础。它需要：使用已定义的评估过程标识出信息安全风险；实施信息安全风险评估的结果；逐步培养管理信息安全风险的能力；实施安全策略和计划，使安全改进结合基于实践的方法。

3. 信息安全风险评估的目标

(1) 了解信息系统的体系结构和管理水平，以及可能存在的安全隐患。

(2) 了解信息系统所提供的服务及可能存在的安全问题。

(3) 了解其他应用系统与此信息系统的接口及相应的安全问题。

(4) 网络攻击和电子欺骗的模拟检测和预防。

(5) 找出目前的安全控制措施与安全需求的差距，并为其改进提供参考。

4. 风险评估的过程

(1) 信息资产评估。使用信息资产的识别过程中得到的信息，就可以为机构中每项信息资产的价值指定权重分数。根据机构的需要，使用的数字可以不同。一些团体使用 1～100 的权重分数，其中 100 代表在几分钟内就会使公司停止运转的信息资产。还有的团体使用 1～10 的权重分数，或者用 1、3 和 5 代表低、中和高价值的资产。也可以根据自己的需要建立权重值。

(2) 风险的确定。信息资产风险的计算公式如下：

风险＝信息资产的价值(或影响)×出现漏洞的可能性－已控制风险的比例＋不确定因素

例如，信息资产 A 的价值是 50，有 1 个漏洞，漏洞 1 出现的可能性是 1.0，当前没有控制风险，估计该假设和数据的准确率为 90%。信息资产 B 的价值是 100，有 2 个漏洞，漏洞 2 出现的可能性是 0.5，当前已控制的风险比例是 50%；漏洞 3 出现的可能是 0.1，当前没有控制风险，估计该假设和数据的准确率为 80%。这 3 个漏洞的风险等级分别如下：

$$\begin{aligned}
\text{资产 } A\text{：漏洞 1 的风险等级} &= (50\times 1.0)(1-0\%+10\%)\\
&= (50\times 1.0)\times 1-(50\times 1.0)\times 0\%+(50\times 1.0)\times 10\%\\
&= 50+0+5=55\\
\text{资产 } B\text{：漏洞 2 的风险等级} &= (100\times 0.5)(1-50\%+20\%)\\
&= (100\times 0.5)\times 1-(100\times 0.5)\times 50\%\\
&\quad +(100\times 0.5)\times 20\%\\
&= 50-25+10=35\\
\text{资产 } B\text{：漏洞 3 的风险等级} &= (100\times 0.1)(1-0\%+20\%)\\
&= (100\times 0.1)-(100\times 0.1)\times 0\%+(100\times 0.1)\times 20\%\\
&= 10-0+2=12
\end{aligned}$$

(3) 识别可能的控制。对于每一个威胁及其残留风险的相关漏洞而言，应该建立一份控制计划的初步列表。残留风险是指使用了现有的控制方法后信息资产残留的风险。控制的一种特殊应用是访问控制，它主要控制用户进入机构信息区域。这些区域包括信息系统、物理限制区域，如机房、甚至整个机构。访问控制通常由政策、计划和技术组成。访问控制有许多方法，访问控制可以是强制的、非任意的和任意的。每种方法都针对一组控制，以便管理对某类信息或信息集合的访问。

(4) 记录风险评估的结果。在风险评估过程结束时，将得到一份很长的信息资产列表，其中包含这些信息资产的各种数据。到目前为止，这个过程的目标是识别机构中有某些漏

洞的信息资产，并将它们列出来，依照最需要保护的顺序划出等级。在准备这个列表时，需要收集和存储资产、资产面临的威胁和包含的漏洞等许多信息，还应收集已有控制的一些信息。漏洞风险等级表如表 1.1 所示。表中列出了每项易受攻击的资产，显示了权重因子分析表中此项资产的价值。在这个例子中，数字从 1～100，并列出了每个不可控的漏洞及其出现的可能性，并计算出风险等级因子。从表中可以看出，最大的风险来自易受攻击的邮件服务器。尽管由客户服务电子邮件所代表的信息资产的影响等级仅为 55，但是硬件相对较高的故障率使它成为最紧迫的问题。

表 1.1　漏洞风险等级表

资　　产	资产影响或相关价值	漏　　洞	漏洞出现的可能性	风险等级因子
通过电子的客户服务请求(输入)	55	由于硬件故障而导致电子邮件中断	0.2	11
通过 SSL 客户订单(输入)	100	由于 Web 服务器硬件故障而导致订单丢失	0.1	10
通过 SSL 的客户订单(输入)	100	由于 Web 服务器或 ISP 服务故障而导致订单丢失	0.1	10
通过电子的客户服务请求(输入)	55	由于 SMTP 邮件转发攻击而导致电子邮件中断	0.1	5.5
通过电子的客户服务请求(输入)	55	由于 ISP 服务失败而导致电子邮件中断	0.1	5.5
通过 SSL 的客户订单(输入)	100	由于 Web 服务器拒绝服务攻击而导致订单丢失	0.025	4.5
通过 SSL 的客户订单(输入)	100	由于 Web 服务器软件故障而导致订单丢失	0.01	1

既然完成了风险识别过程，那么此过程的文件包含的内容应该是什么呢？为风险识别规划的过程应该指明此报告的作用、负责准备报告的人员以及检查这些报告的人员。漏洞风险等级表是风险管理过程下一阶段(评估并控制风险)的初始工作文件。表 1.2 显示了信息安全项目准备的标本表。

表 1.2　风险识别及评估成果

成　果	用　途
信息资产分类表	集合信息资产以及它们对机构的影响或价值
权重标准分析表	为每项信息资产分配等级值或影响权重
漏洞风险等级表	为每对无法控制的资产漏洞分配风险等级

5. 风险控制策略

当机构管理人员发现信息安全威胁的风险产生了竞争劣势时，就通过信息技术和信息安全利益团体来控制风险，一旦该团体建立了漏洞等级表，就可以选择 4 项基本策略中的一项来控制这些漏洞产生的风险。这 4 个策略如下：

(1) 采取安全措施，消除或者减少漏洞的不可控制的残留风险(避免)。

(2) 将风险转移到其他区域，或者转移到外部(转移)。

(3) 减少漏洞产生的影响(缓解)。

(4) 了解产生的后果,并接受没有控制或者缓解的风险(接受)。

避免是试图防止漏洞被利用的风险控制策略。这是一种首选的方法,通过对抗威胁、排除资产中的漏洞、限制对资产的访问和加强安全保护措施来实现。

转移是将风险转移到其他资产、其他过程或其他机构的控制方法。它可以通过重新考虑如何提供服务、修改部署模式、外包给其他机构、购买保险或与提供商签署服务合同来实现。这样,机构就可以将管理复杂系统的风险转嫁给对处理这些风险有经验的另一个机构。使用专业合同的一个好处是提供商对灾难恢复负责,并通过服务级别协定来保证服务器和网站的可用性,但是外包并非不存在风险。信息资产的所有者、IT 管理人员和信息安全组要保证外包合同中的灾难恢复要求足够多,并在进行恢复工作前得到满足。如果外包商没有履行合同条款,结果就可能比预计的要糟糕得多。

缓解是一种控制方法,它试图通过规划和预先的准备工作,来减少漏洞造成的影响。这种方法包括 3 类计划,即事件响应计划(IRP)、灾难恢复计划(DRP)和业务持续性计划(BCP)。每种计划都取决于尽快检测和响应攻击的能力,依赖于其他计划的建立和质量。缓解起源于早期发现的攻击和机构快速、高效的响应能力缓解策略如表 1.3 所示。

表 1.3 缓解策略

计 划	描 述	实 例	何时使用	时间范围
事件响应计划(IRP)	在事件(攻击)进行过程中机构采取的行动	• 灾难发生期间采取的措施 • 情报收集 • 信息分析	当事件或者灾难发生时	立即并实时做出响应
灾难恢复计划(DRP)	发生灾难时的恢复准备工作;灾难发生之前及过程中减少损失的策略;逐步恢复常态的具体指导	• 丢失数据的恢复过程 • 丢失服务的重建过程 • 结束过程来保护系统和数据	在事件刚刚被确定为灾难后	短期恢复
业务持续性计划(BCP)	当灾难的等级超出 DRP 的恢复能力时,确保全部业务继续动作的步骤	• 启动下级数据中心的准备步骤 • 在远程服务位置建立热站点	在确定灾难影响了机构的持续运转之后	长期恢复

与缓解不同,接受风险是选择对漏洞不采取任何保护措施,接受漏洞带来的结果。这可能是一个明智的业务决策,也可能不是。这种策略的有效使用只有在机构进行以下工作之后:

(1) 确定了风险等级。

(2) 评估了攻击的可能性。

(3) 估计了攻击带来的潜在破坏。

(4) 进行了全面的成本效益分析。

(5) 评估了使用每种控制的可行性。

(6) 认定了某些功能、服务、信息或者资产不值得保护。

这种控制,或者说不进行控制,是基于这样一种结论:保护资产的成本抵不上安全措施的开销。

如果机构中每个已识别的漏洞都通过接受策略来处理,就说明该机构没有能力采取安

全措施，总体上对安全是漠不关心的。机构不能将无知当作一种理由，以不知道有责任保护员工客户的信息为借口，来避免被起诉。管理人员不能认为，如果他们不保护信息，攻击者就会觉得通过攻击不会获得有价值的信息。

理解了用于控制风险的策略，下面需要选择正确的策略，防范特定信息资产中的特定漏洞。

6. 选择风险控制策略

风险控制要为每个漏洞选择 4 个风险控制策略中的一个。在信息系统设计好后，就可弄清这个受保护的系统是否存在漏洞，是否可以利用。如果答案是肯定的，并且存在威胁，就要检查攻击者可以从成功的攻击中获得什么。要确定这个风险是否能接受，应估算该风险会对机构造成多大的损失。

下面介绍选择策略的一些规则作为进一步的指导。在计算不同策略的益处时，要注意威胁的等级和资产的价值在策略选择中有着非常重要的作用。

存在漏洞(缺陷或者缺点)：实现安全控制，来减少漏洞被利用的可能性。

(1) 漏洞可以利用。应用分层保护、结构设计和管理控制，使风险降至最小或者防止风险发生。

(2) 攻击者的开销少于收益。通过保护来增加攻击者的成本(如使用系统控制限制系统用户能够访问的资源，从而明显减少攻击者的收益)。

(3) 可能的损失非常大。应用设计原理建筑设计、技术和非技术保护手段，来限制攻击的范围，从而减少可能的损失。

一旦实现了控制策略，就应对控制效果进行监控和衡量，来确定安全控制的有效性，估计残留风险的准确性。注意这个循环不会终止，只要机构继续运转，这个过程就会继续。并不是每个机构都有共同的意向和预算，通过应用控制对每个漏洞进行管理。所以，每个机构必须定义其可能碰到风险的等级。

风险可接受程度的定义如下：当机构评估绝对安全与无限制访问之间达到平衡时愿意接受的风险的级别和种类。例如，一家金融服务公司由政府管理，比较保守，希望应用各种合理的控制，甚至一些带有攻击性的控制来保护它的信息资产。另一个不由政府管理的公司也比较保守，希望避免在漏洞对完整性的损害方面进行负面报道。因此防火墙经销商可能制定比正常情况严厉得多的一组防火墙规则，因为在客户看来，被攻击后的消极结果是灾难性的。其他机构可能因为无知而带来非常危险的风险。针对风险，一个合理的方案是平衡暴露漏洞可能造成的损失和控制这些漏洞的开销。

即使机构尽可能地控制各种漏洞，仍然存在一些风险未能够完全排除、缓解或规划，这称为残留风险。换言之，残留风险是：

(1) 降低了通过安全措施减小威胁效果的一种威胁。

(2) 降低了通过安全措施减少漏洞效果的一种漏洞。

(3) 降低了通过安全措施保护资产价值的效果的一种资产。

必须在机构内部判定残留风险的重要性，尽管这是违反直觉的，信息安全的目标并不是将残留风险降低为 0，而是将残留风险保护在机构可以控制的范围内。如果决定者发现有未受控制的风险，而各利益团体内部的权威机构决定不再理睬残留风险，这个信息安全计划就达到了它的主要目的。