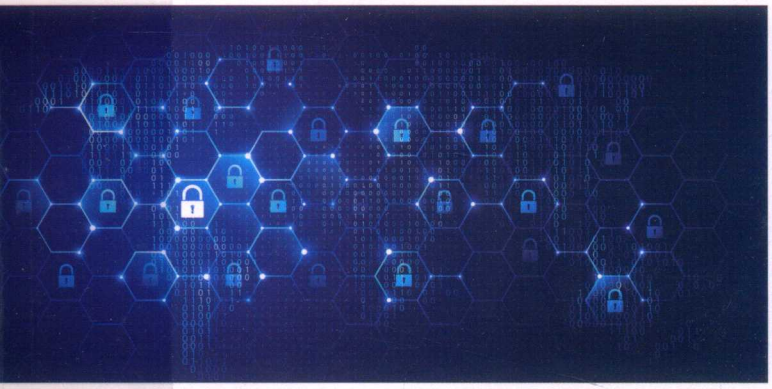
信息安全管理

薛丽敏 韩 松 林晨希 张伟伟 文 俭 编著



国防工业出版社
National Defense Industry Press

信息安全管理

薛丽敏　韩　松　林晨希　张伟伟　文　俭　编著

国防工业出版社

·北京·

内容简介

本书以构建信息安全管理体系为框架，全面介绍了信息安全管理的基本概念、信息安全管理体系以及信息安全管理的各项内容和任务。本书从信息安全管理的产生和基本内涵入手，内容涵盖了信息安全管理体系的建立与实施、信息安全风险管理、组织与人员管理、环境与实体安全管理、软件使用安全管理、应用系统开发安全管理、运行与操作安全管理、安全应急响应管理、灾难恢复、信息安全测评认证管理等，最后对信息安全等级保护和信息安全管理效能评估进行了系统的探讨。

本书可作为信息安全相关专业的本科生及研究生教材，或信息管理与信息系统专业及计算机相关专业的参考书，也可作为信息化管理人员、安全管理人员、网络与信息系统管理人员、IT咨询顾问与IT技术人员的参考手册和培训教材。

图书在版编目(CIP)数据

信息安全管理/薛丽敏等编著. —北京：国防工业出版社，2019.4
ISBN 978-7-118-11798-1

Ⅰ. ①信… Ⅱ. ①薛… Ⅲ. ①信息系统-安全管理 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2019)第053703号

※

国防工业出版社出版发行
（北京市海淀区紫竹院南路23号 邮政编码100048）
三河市天利华印刷装订有限公司印刷
新华书店经售
*
开本 787×1092 1/16 印张 11½ 字数 278千字
2019年4月第1版第1次印刷 印数 1-2000册 定价 46.00元

（本书如有印装错误，我社负责调换）

国防书店：(010)88540777 发行邮购：(010)88540776
发行传真：(010)88540755 发行业务：(010)88540717

前　言

目前，人类社会已经昂首阔步迈进了信息时代。甚至有人说，我们可能不需要阳光，但绝对离不开信息。信息已经渗透到了人类社会的每一个角落，融入了人们生活的每一个细节，就像一只无形的大手渗透于社会各行各业之中，推动着社会的进步。与此同时，随着信息技术在军事领域的发展，围绕信息、知识和智能较量的信息战已无处不在。因此，信息安全已成为国家安全的基础和关键。信息安全发展至今，已经从强调针对信息及信息系统的各种威胁所采取的必要措施，发展到强调信息系统的保护、检测和恢复能力的信息安全保障，其本质是从被动的、静态的措施，到主动的、动态的能力。在信息安全保障的三大要素人员、技术和管理中，管理要素的地位和作用越来越受到重视。如同科学管理和信息控制方法是指挥着信息这只大手的大脑中枢神经一样，信息安全作为信息科学的一个重要组成部分，管理与控制也是信息安全领域的核心思想。

信息安全的威胁来自于内部破坏、外部攻击、内外联合进行的破坏以及自然危害等，从信息安全管理体系的高度来全面构建和规范信息安全管理，对信息与信息系统可能面临的威胁、脆弱性进行分析，并依据风险评估的结果及等级保护等一整套信息安全管理思想和方法，为信息系统选择有针对性的安全措施，规避、转移和降低风险，妥善应对可能发生的风险，并将风险控制在可接受的范围内，将有效地保障我国的信息安全。

信息安全管理是一个十分重要的课题，其发展对信息安全人才的培养提出了新的需求。本书是将信息安全管理作为一个系统工程，综合集成于一体进行研究、探讨和阐述的，力求由浅入深、内容简练、体系完整。同时，本着“基础、前沿、应用”兼顾的思想，以信息安全管理基本理论为基础，分别对信息安全管理各项活动和过程的思想与方法展开论述，使读者能够在系统准确地把握信息安全管理思想的基础上，正确有效地运用信息安全管理的方法和技术，分析解决实际问题。

全书由薛丽敏负责统稿，其中第 1 章由薛丽敏编写，第 2、3、8、10 章由韩松编写，第 4、5、9、11 章由张伟伟编写，第 6、7、12 章由林晨希编写。

在编写本书时，直接或间接地引用了许多专家、学者的文献和著作，在此向他们表示衷心的感谢！

信息安全学科内容广泛，发展迅速，信息安全管理及相关内容也在不断更新。由于作者水平有限，书中难免存在不足和错误之处，敬请读者批评指正。

编著者

2017 年 10 月

目　录

第1章 概 论

随着信息技术的不断发展及其广泛应用,国防、通信、能源、交通、金融等对信息资源的依赖程度越来越高,没有各种信息的支持,现代社会将无法存在和发展。但是,信息资源和信息化在为人类社会提供各种便利的同时,也带来了一定的安全风险。由于环境的开放性和信息系统自身缺陷的存在,信息资源同时面临着来自内部和外部两个方面的威胁。信息资源和信息化在为人类社会提供各种便利的同时,也带来了信息安全风险。因此,根据信息安全风险的来源和层次,有针对性地采取技术、管理和法律等措施,构建立体的、全面的信息安全管理体系,保证信息系统和信息资源的安全,已成为共识。

1.1 信息安全管理产生的背景和发展现状

信息安全管理是随着信息和信息安全的发展而发展的。在信息社会中,一方面信息已经成为人类的重要资产,在政治、经济、军事、教育、科技、生活等方面发挥着重要作用,另一方面由于计算机技术的迅猛发展而带来的信息安全问题正变得日益突出。由于信息具有易传播、易扩散、易损毁的特点,信息资产比传统的实物资产更加脆弱,更容易受到损害,这样将使组织在业务运作过程中面临巨大的风险。这种风险主要来源于组织管理、信息系统、信息基础设施等方面的固有薄弱环节和漏洞,以及大量存在于组织内外的各种威胁,因此对信息系统需要加以严格管理和妥善保护,信息安全管理也随之产生。

1.1.1 信息、信息战与信息安全

1. 信息

信息是指音讯、消息、通信系统传输和处理的对象,泛指人类社会传播的一切内容。人们通过获得、识别自然界和社会的不同信息来区别不同事物,得以认识和改造世界。在一切通信和控制系统中,信息是一种普遍联系的形式。1948 年,数学家香农在“通信的数学理论”的论文中指出:“信息是用来消除随机不定性的东西”。创建一切宇宙万物的最基本的万能单位是信息。

通常情况下,可以把信息理解为消息、信号、数据、情报和知识。信息本身是无形的,借助于信息媒体以多种形式存在或传播。它可以存储在计算机、磁带、纸张等介质中,也可以记忆在人的大脑里,还可以通过网络、打印机、传真机等方式进行传播。

对现代企业和组织来说,信息也是一种资产,不仅包括与计算机、网络相关的数据、资料,还包括专利、标准、商业档案、文件、图样、统计数据、配方、报价、规章制度、财务数据、工艺、计划、资源配置、管理体系、关键人员等。就如其他重要的商业资产那样,信息资产也具有重要的价值,因而同样需要进行妥善保护。

所有的组织都有各自处理信息的形式,如银行、保险和信用卡公司需要处理金融信息,企业、商家需要处理消费者信息,政府管理部门需要处理、存储公众和机密信息。无论这些信息采用什么样的处理、存储和共享方式,都需要对信息加以安全、妥善的保护,不仅要保证信息处理

和传输过程是可靠、有效的,而且要求重要的敏感信息是机密的、完整的和真实的。为达到这样的目标,必须采取一系列适当的信息安全控制措施以抵御一系列威胁,保障业务的持续性,最大限度地降低安全威胁的影响,减少业务和系统的损失。由于信息是有生命周期的,因此,从安全保护的角度去考察信息资产,决不能只停留在静态的一个点或者一个层面上,而是要考虑到从其创建或诞生,到使用或操作,再到存储或传递,直至销毁或丢弃整个生命周期中各个环节和各个阶段。

2. 信息战

随着信息技术在军事领域的应用和发展,信息和信息武器装备在作战中发挥着越来越重要的作用,尤其是海湾战争、科索沃战争和伊拉克战争的实践,使各国军事理论界都加快了对信息战的研究。

1976 年,美国军事理论家汤姆·罗那在为波音信息系统拟定的一份题为《武器系统与信息战争》的研究报告中,首次使用了"信息战争"的概念,并指出信息战争是决策系统之间的斗争。1984 年,美国空军开始使用"信息战斗"一词。1985 年,美国海军电子司令部副司令加洛塔少将在美国《电子防御杂志》上发表了题为"电子战与信息战"的论文。随后,美国主管 C^3I 的助理国防部长兼国家电信系统安全保密委员会主席莱瑟姆撰文指出:"信息时代的主要武器是信息,谁掌握了信息,谁就拥有了作战力量的基础。"1989 年,美国情报与电子战专家提出了计算机病毒对抗理论。1989 年,我国专家也提出了"计算机病毒武器"概念。1985 年,沈伟光开始研究信息战,并在 1990 年出版了世界上第一部有关信息战的专著——《信息战》一书。他在书中指出:"信息战,广义上是指对垒的军事集团抢占信息空间和争夺信息资源的战争,狭义上是指战争中交战双方在信息领域的对抗。"

目前,信息战已成为美国、俄罗斯、日本、欧盟各国军方关注的焦点,其含义在各国军事学术界也是众说纷纭,现将部分观点作简要介绍。

美国认为:信息战即心理战;信息战是攻击对方认知系统与反应系统的战争;信息战是信息干扰和信息防护;信息战是计算机空间战;信息战是夺取"信息霸权"的较量,并在此基础上提出了"网络中心战"。

俄军把信息战称为"第六代战争",俄军总参参谋学院的军事理论家认为,信息战是敌对双方为争夺和保持信息优势而采取的解决冲突的一种手段。

日本的军事理论家们对信息战争的研究投入了很大精力。他们认为,信息战是在和平时期、危机爆发时、危机加深时、爆发战争时、战争进行中、战争结束时和战后重建时的各个时期,在战略、战役、战术层次上,在竞争者、对手和敌我之间,使用各种手段以达成既定目标的信息行动。信息战将成为 21 世纪典型的作战形式,信息战包括了指挥控制战、以信息为基础的作战、电子战、心理战、"黑客"战、经济信息战和网络空间战 7 种作战类型。

上述各家都是从某一角度或某一方面对信息战的含义作了界定。实际上,信息战已成为一个多义词,根据美国国防部在 1996 年 6 月公布的《军事尖端技术一览表》中罗列的具体信息战形式,信息战包括电子战、实质性摧毁、欺骗、心理战等传统样式。一切指向信息、以信息为基础的过程、信息系统和信息基础设施的斗争都是信息战。网络战、电脑战、"黑客"战、指挥控制战等都是由现代信息技术发展而导引出的具体的信息战形式,是在具体的信息媒体、流动空间、特殊技术手段、特定目标下遂行的对抗形式。也有人认为:"信息战包含了战争或作战条件下的电子战、网络战、导弹战、情报战和心理战等,其核心内容是指挥控制战。

我国专家们认为,信息战是使用信息技术和信息化武器装备,在保护己方的信息和信息系

统的同时,对敌方的信息和信息系统实施打击的一种作战样式。其实质是作战双方为争夺信息的获取权、控制权和使用权而展开的斗争。信息战产生于人类社会形态由工业社会向信息社会的过渡期,是社会信息化和军事信息化的初期阶段在军事上的一种反映。信息战是武器装备初期信息化带来的一种结果,是信息化战争的核心。

信息战的基本形式分为信息进攻和信息防御两种:信息进攻是综合运用各种软/硬杀伤、破坏手段,对敌信息系统实施侦察、干扰、欺骗、侵入、阻断、破坏和摧毁等行动;信息防御是为破坏或削弱敌信息进攻,保障己方使用信息的自由,综合利用各种手段,对己方信息系统实施保护的措施与行动。工业时代战争所释放的能量主要是热能,而且是无节制的,其附带性毁伤巨大,信息时代的战争则是热能和智能相结合的能量释放形态,能量的释放有控制性,而且更有针对性,使之与战争的目的更加符合,从而更有利于战争目的的实现。

信息战的核心力量是信息、知识和智能,信息战是信息、知识和智能的较量。信息战离不开信息化、智能化的武器装备和信息化军队。信息战的筹划和组织已从完全以人为主发展到日益依赖技术手段的人机结合,对军人知识水平的要求也更高。从信息优势到最终转化为决策优势,是信息、知识和智能较量的结果。

信息战按其所凭借的信息系统的信息化水平,可划分为以下3个层次。

(1) 网络战。网络战对应于认知的信息层,以网络化信息系统为基础,将信息和网络化信息系统作为主要攻防对象,以获取信息优势为目的。

(2) 知识战。知识战对应于认知的知识层,以知识化信息系统为基础,将知识和知识化信息系统作为主要攻防对象,以获取知识优势为目的。

(3) 智慧战。智慧战对应于认知的智慧层,以智慧化信息系统为基础,将智慧和智能化信息系统作为主要攻防对象,以获取智慧优势为目的。

知识战是信息战的核心,也是信息战的实质所在。

综上所述,信息战是指不以通过物质和能量的战争手段、大规模杀伤敌人有生力量为目的,而以信息优势的争夺和对抗为主导,以保护与增强本方侦察、指挥、控制系统,削弱、摧毁敌方指挥、控制系统为主要目的,从而使敌方不能作出决策或作出错误决策而丧失战斗力的战争。因此,信息战的要点是:保证己方的信息安全,打击破坏敌方的信息安全,力图使敌方的信息系统丧失能力,信息不可信任,心理受到创伤,同时保护己方不受类似损失。

随着信息理论与信息安全技术的日益发展,理论上信息安全应该得到有效保障,然而现实情况是信息安全形势日益脆弱和恶化。造成这一现象的根本原因是当今信息环境日益开放,网络日益普及,管理日趋复杂和困难,随着网上用户的日益增多,潜在的黑客、攻击者也日益增多。各信息大国都高度重视,并投入巨资研究新一代国际互联网,许多国家甚至直接征召黑客入伍,网络战场上的争夺日趋激烈。

3. 信息安全

事实上,信息安全的课题以及信息战的攻击和防御,古来有之。农业社会生活节奏缓慢,信息的产生、加工、传播周期漫长,传送距离有限,因而信息安全造成的破坏规模和范围也就有限。

工业社会的后期虽然有了计算机,20年前也只有大型的计算机主机,所运行的是少量的、集束型的计算题。用户需要排时进入计算机机房上机和取得运算结果。即使用户通过有限的终端上机,那也只是缺乏智能的哑终端(Dumb Terminal),充其量是一个连接主机的远端输入/输出装置,功能有限。整个系统的运行完全依赖于主机的工作环境和在主机上的操作。又因为大型机的操作极为复杂和繁复,整机的操作和管理只能由经过长期训练和通过考核的少数专业

人士担任,这些人的背景都经过审核,管理阶层几乎可以每日面对面地和他们接触。在这种封闭的“玻璃房”环境中工作,监测和管理与传统的工业管理并无太大的区别。由于软件开发环境并不完善,开发工具必须在昂贵的特定开发环境中实现,因此能够接触软件开发的人员数目也很有限。这个时期的信息安全主要表现在通信安全方面,即在通信过程中要保证所传送的信息不被捕获(或分析)、不被篡改、不被伪造。

20 世纪 80 年代,个人计算机和网络日益普及,80 年代的信息安全问题表现在计算机单机的安全方面,包括访问控制等;90 年代的信息安全问题则主要表现在网络安全方面,远端的黑客和攻击者完全可以通过自身的终端,经过网络的放大效应,实施隐蔽的、实时的、自制的恶意代码攻击。由于互联网将分离的个别网络连成大网,一处受害、受感染,会迅速波及全网。1988 年 11 月 2 日晚,美国国防战略 C^4I 系统的主控制中心和各级指挥控制中心,相继遭受“莫里斯蠕虫”攻击,约 8500 台计算机受损,6000 台计算机不能工作。病毒不到 10h 就席卷东西两岸,直接损失上亿美元,而目前一个病毒的传播速度只要 30min 就可席卷全球。

信息技术的发展带动了全球信息化的发展,从而使信息基础设施成为社会基础设施中必不可少的关键部分,随着 Internet 的广泛普及,在给人们带来巨大便利的同时,信息安全问题也日益突出。具体表现有:黑客攻击搅得全球不安,已由零散的个人行为发展成为有组织的团队行为;计算机病毒在网上肆虐;白领犯罪造成巨大商业损失;数字化能力的差距造成世界上不平等竞争,信息战阴影威胁着数字化和平。正所谓“Internet 最大的好处是将你和所有人都连在一起,Internet 最大的坏处也是将你和所有人都连在一起”。

因此,许多专家认为“威胁是客观存在的事实”。信息战是因特网发展的一个必然结果,是人们生活在信息社会中付出的代价之一。信息战的要点之一就是保证己方的信息安全,打击破坏敌方的信息安全。

信息安全的含义大致可以分成两大类:一类是指具体的信息技术系统的安全;另一类是指某一特定信息体系(如一个国家的银行信息系统、军事指挥系统等)的安全。从广义上,信息安全是指:“一个国家的社会信息化状态和信息技术体系不受外来的威胁与侵害。”狭义上,信息安全可以定义为:“保护信息及信息系统在信息存储、处理、传输过程中不被非法访问或修改,而且对合法用户不发生拒绝服务。信息安全包括检测(探测)、记录、对抗此类威胁所必要的措施。”信息安全是一个广泛而抽象的概念,不同领域不同方面对其概念的阐述都会有所不同。

信息作为一种资产,是企业或组织进行正常商务运作和管理不可或缺的资源。从最高层次来讲,信息安全关系到国家的安全;对于组织机构来说,信息安全关系到正常运作和持续发展;就个人而言,信息安全关系到个人隐私和财产的安全。无论是个人、组织还是国家,保护关键的信息资产的安全性都是非常重要的。信息安全的任务,就是要采取措施(技术手段及有效管理)让这些信息资产免遭威胁,或者将威胁带来的后果降到最低,以此维护组织的正常运作。

随着人类文明的发展与进步,信息处理的方法与技术也在不断发展,从最原始的语言文字,到古代文字、纸张的发明,再到现代通信、计算机与网络技术的普遍应用,信息的储存、交流、传输、处理的技术与方法越来越多,越来越复杂,信息储存的媒体也随之增多。信息量正在呈几何级数增长,信息的传播容量不断增加、传播速度不断加快、信息资产所面临的安全威胁也在不断地增加,因而信息安全技术也得到了相应的发展。当然在不同的发展时期,信息安全的侧重点与信息安全的控制方式与手段也不尽相同。从产生到现在,信息安全的发展经历了以下几个过程。

(1) 通信保密:20 世纪 60 年代以前,主要是在通信的收发双方加入了加密这一个环节。

(2) 计算机安全:20 世纪 70 年代至 80 年代,主要研究信息的机密性、完整性、可用性,还有安全 OS 技术。

(3) 网络信息安全:20 世纪 90 年代后,主要研究网络上的信息、信息对抗、虚拟专用网 VPN、公钥基础设施 PKI 和风险评估等。

(4) 构造信息安全基础设施等保障体系阶段:21 世纪,主要为数据备份与灾难恢复技术、国际联动的安全应急响应等。

可以看出,信息安全发展至今,从强调对抗针对信息及信息系统的各种威胁所必要的措施,到强调信息系统的保护、检测和恢复能力,即信息安全保障(Information Assurance,IA),其本质是从被动的、静态的措施,到主动的、动态的能力。因此,信息安全保障是信息安全理论的重要发展,其目标是使系统从组建到运行的整个生命周期都满足安全需求。

1.1.2　信息安全管理产生的时代背景

目前,信息安全已发展到了信息的可靠性、可用性、可控性、完整性和不可抵赖性等更新、更深层次的领域。这些领域内的相关技术和理论都是信息安全所要研究的领域。国际标准化组织(ISO)对信息安全的定义为:"在技术上和管理上为数据处理系统建立的安全保护,保护计算机硬件、软件和数据不因偶然和恶意的原因而遭至破坏、更改和泄露。"

长久以来,很多人都会陷入技术决定一切的误区当中,尤其是那些出身信息技术行业的管理者和操作者。最早的时候,人们把信息安全的希望寄托在加密技术上,认为一经加密,安全性能就会有保障。随着网络的发展和普及,一段时期又常听到"防火墙决定一切"的论调。当更多的安全问题出现时,入侵检测系统(Intrusion Detection System,IDS)、公钥基础设施(Public Key Infrastructure,PKI)、虚拟专用网(Virtual Private Networks,VPN)等新的技术应用被接二连三地提了出来,但无论怎么变化,还是离不开技术统领信息安全的狭隘思路。可这样的思路能够真正解决安全问题吗?也许可以解决一部分,但却解决不了根本问题。

实际上,对安全技术和产品的选择运用,只是信息安全实践活动中的一部分,是实现安全需求的手段。信息安全更广泛的内容,还包括制定完备的安全策略,通过风险评估来确定需求,根据需求选择安全技术和产品,并按照既定的安全策略和流程规范来实施、维护和审查安全控制措施。归根到底,信息安全并不是技术过程,而是管理过程。

随着信息安全理论与技术的发展,信息保障的概念得以提出,并得到一致认可,而在信息保障的三大要素(人员、技术和管理)中,管理要素的作用和地位越来越受到重视,在信息保障的概念中,信息安全一般包括实体安全、运行安全、信息安全和管理安全 4 个方面的内容。

(1) 实体安全:保护计算机设备、网络设施以及其他通信与存储介质免遭地震、水灾、火灾、有害气体和其他环境事故(如电磁污染等)破坏的措施和过程。

(2) 运行安全:为保障系统功能的安全实现,提供一套安全措施(如风险分析、审计跟踪、备份与恢复、应急措施)来保护信息处理过程的安全。

(3) 信息安全:防止信息资源的非授权泄露、更改、破坏,或信息被非法系统辨识、控制和否认,即确保信息的机密性、完整性、可用性、不可否认性和可控性。

(4) 管理安全:通过信息安全相关的法律法令和规章制度以及安全管理手段,确保信息系统安全生存和运营。

信息安全的建设是一个系统工程,它需要对信息系统的各个环节进行统一的综合考虑、规划和构架,并时时兼顾组织内外不断发生的变化,任何环节上的安全缺陷都会对系统构成威胁。

信息安全体系结构的理论基础是整体论、系统论和“木桶”理论。

整体论强调整体功能大于部分功能和，主要处理整体与部分的关系。整体功能的发挥依赖于各部分的密切配合与通力协作，即整体中各部分要有自己强大的功能，各部分之间要有无缝的连接。在整个安全防护中，功能相对较弱的部分以及各部分之间的协作程度对系统的整体安全防护起着至关重要作用，要有针对性地加以改进。

系统论强调系统中各元素功能的密切协作。系统元素的协作性是系统功能的基础，任何单一元素或一部分元素的组合都不具有系统功能。在信息安全系统中，所有各部分的协作联动是保障安全的最佳结构。

“木桶”理论的含义是：一个木桶能不能容水，能容多少水，除了看最短木板之外，还要看这个木桶是否有坚实的底板、木板之间是否有缝隙。正是这谁也不太重视的底板，决定这只木桶能不能容水，能容多大重量的水。这底板正是信息安全的基础，即信息安全体系结构（Information Security Architecture）、制度建设和流程管理。木桶能否有效地容水，除了需要坚实的底板外，还取决于木板之间的缝隙，木桶是否有缝隙是木桶能否容水的关键。对于一个安全防护体系而言，其不同产品之间的协作和联动问题，有如木板之间的缝隙，通常被我们所忽视，但其危害却最深。

由于信息安全是一个多层面、多因素、综合和动态的过程，如果凭着一时的需要，想当然地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。正确的做法是，遵循国内外相关信息安全标准与最佳实践过程，考虑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，建立合理的安全管理体系，从而保证信息资产的安全性。另外，这个安全体系还应当随着环境的变化、业务的发展和信息技术的提高而不断改进，不能一劳永逸、一成不变。因此，信息安全的实现是一个需要完整的技术和管理体系来保证的持续过程。

1.1.3 信息安全管理发展现状

1. 我国信息安全管理现状

目前，我国信息安全管理工作已经全面展开，由于国家的信息安全管理涉及工业、农业、国防、教育、商业及政务等国家建设的全局，于2002年4月15日在北京成立了“全国信息安全标准化技术委员会”，并设立了“信息安全管理工作组”，负责对国家信息安全管理的全局实施集中统一的领导，各省市也成立了相应的组织机构。该组织的成立，标志着我国信息安全标准化工作，步入了“统一领导、协调发展”的新时期，但是我国信息安全管理也还面临着以下问题。

（1）信息安全管理现状仍还比较混乱，实际管理力度不够，政策的执行和监督力度不够。部分规定过分强调部门的自身特点，而忽略了在国际政治经济的大环境下体现中国特色。部分规定没有准确地区分技术、管理和法制之间的关系，以管代法，用行政管技术的做法仍较普遍，造成制度的可操作性较差。

（2）具有我国特点的、动态的、涵盖组织机构、文件、控制措施、操作过程和程序以及相关资源等要素的信息安全管理体系还未建立起来。

（3）具有我国特点的信息安全风险评估标准体系还有待完善，信息安全的需求难以确定，要保护的对象和边界难以确定，缺乏系统、全面的信息安全风险评估和评价体系，以及全面、完善的信息安全保障体系。

（4）信息安全意识缺乏，普遍存在重产品、轻服务，重技术、轻管理的思想。

（5）专项经费投入不足，管理人才极度缺乏，基础理论研究和关键技术薄弱，严重依赖国

外,对引进的信息技术和设备缺乏保护信息安全所必不可少的有效管理和技术改造。

(6) 技术创新不够,信息安全管理产品水平和质量不高,尤其是以集中配置、集中管理、状态报告和策略互动为主要任务的安全管理平台产品的研究与开发还很落后。

(7) 我国现有的一些信息安全管理方面的法律法规层次不高,真正的法律少,行政规章多,结构不合理,不成体系;执法主体不明确,多头管理,政出多门、各行其是,规则冲突,缺乏可操作性,执行难度大,有法难依;数量上不够,内容上不完善,制定周期太长,时间上滞后,往往无法可依;监督力度不够,有法不依,执法不严;缺乏专门的信息安全基本大法,如"信息安全法和电子商务法"等;缺乏民事法方面的立法,如"互联网隐私法""互联网名誉权和网络版权保护法"等,公民的法律意识较差,执法队伍力量薄弱,人才匮乏。

(8) 我国制定的信息安全标准太少,大多沿用国际标准。在实施过程中,缺乏必要的国家监督管理机制和法律保护,致使部分企业或用户不按标准执行,或者执行过程中出现的问题得不到及时、妥善解决。

2. 国外信息安全管理现状

制定发展战略和计划是发达国家一贯的做法。美国、俄罗斯、日本都已经或正在制定自己的信息安全发展战略和发展计划,确保信息安全沿着正确的方向发展。2000年初,美国制定了"计算机空间安全计划",旨在加强关键基础设施、计算机系统和网络免受威胁的防御能力。2000年7月,日本信息技术战略本部及信息安全会议拟定了信息安全指导方针。2000年9月12日,俄罗斯发布了《国家信息安全构想》,明确了保护信息安全的措施。

加强信息安全立法,实现统一和规范管理。以法律的形式规定和规范信息安全工作是有效实施安全措施的最有力保证。制定网络信息安全规则的先锋是各大门户网站,美国的雅虎和美国在线等网站都在实践中形成了一套自己的信息安全管理办法。2000年10月1日,美国的电子签名法案正式生效。2000年10月5日,美国参议院通过了《互联网网络完备性及关键设备保护法案》。日本邮政省于2000年6月8日公布了旨在对付黑客的《信息网络安全可靠性基准》的补充修改方案,提出并制定了有关风险管理的"信息安全准则"指导原则。2000年9月,俄罗斯实施了关于网络信息安全的法律。

加快标准化与系统化管理,在20世纪90年代之前,信息安全主要依靠安全技术手段与不成体系的管理规章来实现。在20世纪80年代末,ISO 9000《质量管理标准》出现并在全世界广泛推广应用,系统管理的思想在其他管理领域也被借鉴与采用,如后来的ISO 14000《环境体系管理标准》、OHSAS 18000《职业安全卫生管理体系标准》,信息安全管理也同样在20世纪90年代步入了标准化与系统化管理的时代。1995年,英国率先推出了BS 7799《信息安全管理标准》,并于2000年被国际标准化组织认可为国际标准ISO/IEC17799,现在该标准已引起许多国家与地区的重视,在一些国家已经被推广与应用,组织贯彻实施该标准可以对信息安全风险进行全面系统的管理,从而实现组织信息安全。

1.2 信息安全管理的内涵

管理是在群体活动中为了完成一定的任务、实现既定的目标、针对特定的对象、按照规定的程序、运用恰当的方法所进行的计划、组织、指挥、协调和控制等一系列活动。信息安全管理贯穿于信息系统从系统规划、设计、建设、运行、维护到报废整个生命周期。