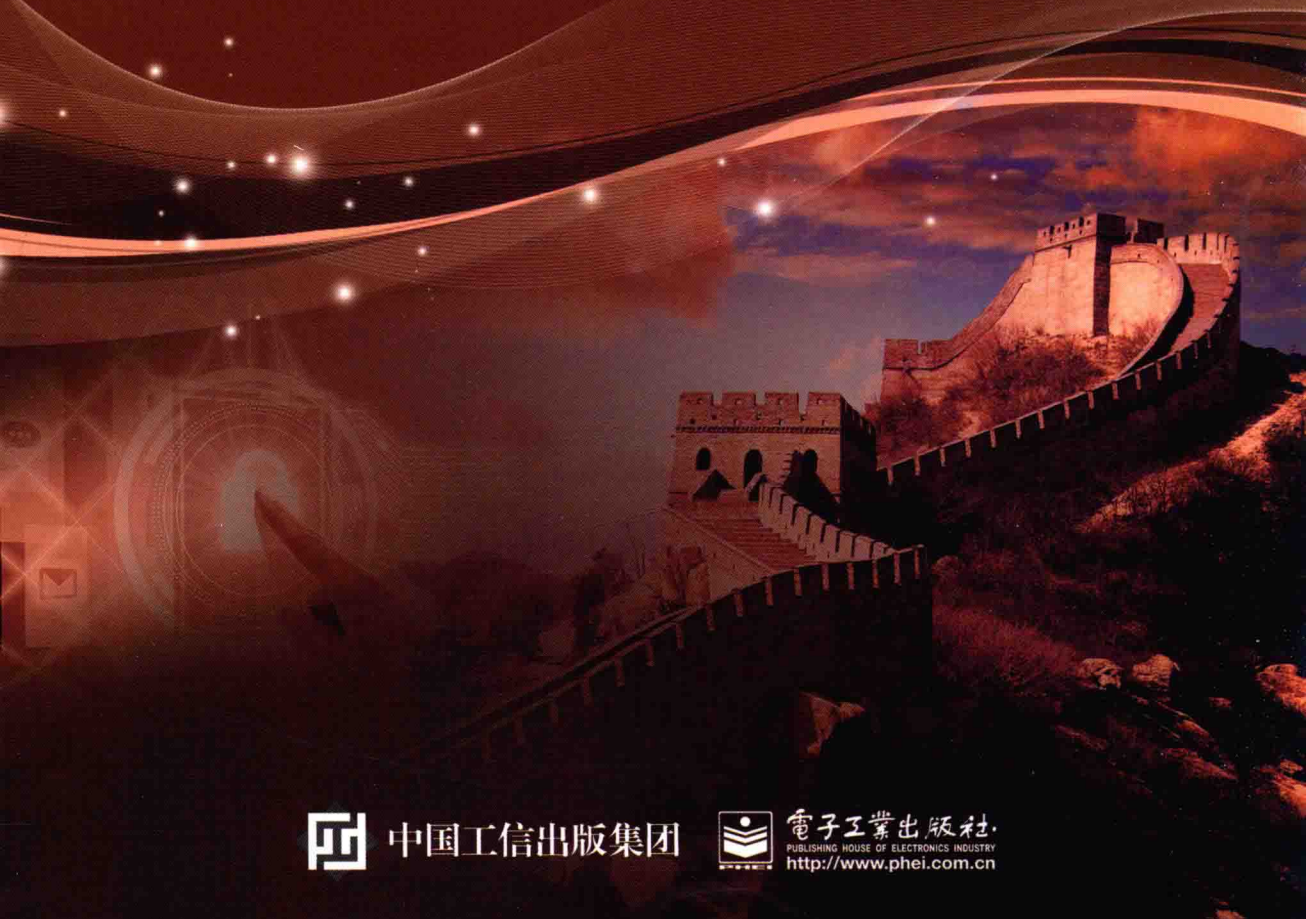
网络空间安全系列教材

信息安全管理

◎ 汤永利　陈爱国　叶 青　闫玺玺　编著



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

网络空间安全系列教材

信息安全管理

汤永利　陈爱国　叶　青　闫玺玺　编著

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

内 容 简 介

本书作为网络空间安全系列教材之一，在广泛吸纳读者意见和建议的基础上，不仅定位于信息安全管理的基本概念、信息安全管理的各项内容和任务的讲解，还适当加入了国内和国际上信息安全技术和管理方面的最新成果，反映出信息安全管理与方法的研究和应用现状。另外，本书力求理论与实际相结合，在部分章节加入实例报告。

本书内容共 8 章。第 1 章是绪论。第 2 章介绍信息安全管理标准与法律法规。第 3 章介绍信息安全管理体系。第 4 章介绍信息安全风险评估。第 5 章介绍信息系统安全测评。第 6 章介绍业务连续性与灾难恢复。第 7 章介绍信息系统安全审计。第 8 章介绍网络及系统安全保障机制。每章后面配有习题以巩固相关知识。

本书可作为高等院校网络空间安全、信息安全专业本科、研究生教材，也可作为相关专业技术人员的参考书目。

图书在版编目（CIP）数据

信息安全管理 / 汤永利等编著. —北京：电子工业出版社，2017.1

ISBN 978-7-121-30137-7

Ⅰ. ①信… Ⅱ. ①汤… Ⅲ. ①信息系统—安全管理Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2016）第 248401 号

策划编辑：袁　玺
责任编辑：郝黎明
印　　刷：三河市良远印务有限公司
装　　订：三河市良远印务有限公司
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：787×1 092　1/16　印张：16.5　字数：494 千字
版　　次：2017 年 1 月第 1 版
印　　次：2017 年 1 月第 1 次印刷
定　　价：42.00 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）88254536。

网络空间安全系列教材

编委会名单

序

随着经济全球化和信息化的发展，以互联网为平台的信息基础设施，对整个社会的正常运行和发展正起着关键的作用。甚至，像电力、能源、交通等传统基础设施的运行，也逐渐依赖互联网和相关的信息系统才能正常运行。网络信息对社会发展有重要的支撑作用。

网络空间是利用全球互联网和计算系统进行通信、控制和信息共享的动态虚拟空间，包括四个要素，分别是网络平台、用户虚拟角色、资产数据和管理活动，是社会有机运行的神经系统，已经成为继陆、海、空、天之后的第五空间。

网络空间面临的威胁也与日俱增。从国际上看，国家或地区在政治、经济、军事等各领域的冲突都会反映到网络空间中，而由于网络空间边界不明确、资源分配不均衡，导致网络空间的争夺异常复杂。另外，网络犯罪和网络攻击也对个人和企业构成严重威胁。在网络中，个人隐私信息泄露并大范围传播的事件已经屡见不鲜，以非法牟利为目的、利用计算机网络进行的犯罪已经形成了黑色的地下经济产业链。如何充分利用互联网对经济发展的推动作用、保护公民和企业的合法权益，同时又要控制其对经济社会发展带来的负面威胁，需要研究和探索更加科学合理的网络空间安全治理模式。正如习近平总书记所言：“没有网络安全，就没有国家安全”。

加强网络空间安全已经成为国家安全战略的重要组成部分。2014 年 2 月，中央网络安全和信息化领导小组成立。2015 年 6 月，国务院学位委员会、教育部决定在“工学”门类下增设“网络空间安全”一级学科，并明确指出需加强“网络空间安全”的学科建设，做好人才培养工作。2016 年 3 月，国务院学位委员会下发通知，明确全国共有 29 所高校获得我国首批网络空间安全一级学科博士学位授权点。6 月，中央网络安全和信息化领导小组办公室、国家发展和改革委员会、教育部、科学技术部、工业和信息化部、人力资源和社会保障部联合发文，《关于加强网络安全学科建设和人才培养的意见》（中网办发文[2016]4 号）指出，网络空间的竞争，归根结底是人才竞争。我国网络空间安全人才还存在数量缺口较大、能力素质不高、结构不尽合理等问题，与维护国家网络安全、建设网络强国的要求不相适应。提出要加快网络安全学科专业和院系建设；创新网络安全人才培养机制；加强网络安全教材建设；强化网络安全师资队伍建设；完善网络安全人才培养配套措施等意见。

网络空间安全主要研究网络空间中的安全威胁和防护问题，即在有敌手的对抗环境下，研究信息在产生、传输、存储、处理、销毁等各个环节中所面临的威胁和防御措施，以及网络和系统本身面临的安全漏洞和防护机制，不仅仅包括传统信息安全所研究的信息的保密性、完整性和可用性，同时还包括构成网络空间基础设施的安全和可信。从宏观层面来看，网络空间安全的研究对象主要包括：全球各类各级信息基础设施的安全威胁；从微观来看，主要对象包括：通信网络、计算机网络及其设备和应用系统中的安全威胁。

数学、信息论、计算复杂性理论等是网络空间安全所依靠的重要理论基础。

网络空间安全的理论体系由三部分组成。一是基础理论体系，主要包括：网络空间理论、

密码学、离散结构理论和计算复杂性理论等；其中，信息的机密性、完整性、可控性、可靠性等是核心，对称加密、公钥加密、密码分析、侧信道分析等是重点，在复杂环境中的可证安全、可信可控及定量分析理论是关键。二是技术理论体系，主要包括网络空间安全保障理论体系，从系统和网络角度，研究和设计网络空间的各种安全保护方法和技术。重点包括：芯片安全、操作系统安全、数据库安全、中间件安全、恶意代码等，从预警、保护、检测到恢复响应的安全保障技术理论。从网络安全角度，以通信基础设施、互联网基础设施等为研究对象，聚焦研究通信安全、网络安全、网络对抗等。三是应用理论体系，从应用角度来看，针对各种应用系统，研究在实际环境中面临的各种安全问题，如 Web 安全、内容安全、垃圾信息等，涵盖电子商务、电子政务、物联网、云计算、大数据等诸多应用领域。

网络空间安全有如下五个研究方向。一是网络空间安全基础，包括：网络空间安全数学理论、网络空间安全体系结构、网络空间安全数据分析、网络空间博弈理论、网络空间安全治理与策略、网络空间安全标准与评测等。二是密码学及应用，包括：对称密码设计与分析、公钥密码设计与分析、安全协议设计与分析、侧信道分析与防护、量子密码与新型密码等。三是系统安全，包括：芯片安全、系统软件安全、虚拟化计算平台安全、恶意代码分析与防护等。四是网络安全，包括：通信基础设施及物理环境安全、互联网基础设施安全、网络安全管理、网络安全防护与主动防御（攻防与对抗）、端到端的安全通信等。五是应用安全，包括：关键应用系统安全、社会网络安全（包括内容安全）、隐私保护、工控系统与物联网安全、先进计算安全等。

中国密码学会教育与科普工作委员会与电子工业出版社合作，共同筹划了这套“网络空间安全系列教材”，主要包括《密码学》、《密码学实验教程》、《公钥密码学》、《应用密码学》、《密码学数学基础》、《密码基础算法》、《典型密码算法 FPGA 实现》、《典型密码算法 JAVA 实现》、《公钥密码算法 C 语言实现》、《密码分析学》、《网络空间安全导论》、《信息安全管理》、《信息系统安全》、《网络空间安全技术》、《网络空间安全实验教程》、《网络攻防技术》、《同态密码学》、《对称密码学》等。希望为信息安全、网络空间安全、网络安全与执法、信息对抗技术等本科专业提供教材，也为密码学、网络空间安全、信息安全等专业的研究生和博士生，以及从事该领域的科研人员提供教材和参考书。为我国网络空间安全教材建设、普及密码知识和网络空间安全人才培养，贡献绵薄之力。

2016 年 12 月

前言

随着人们对信息技术依赖程度的不断加深，信息安全受到了社会的普遍关注。通过技术手段针对性地解决信息安全问题是信息安全防范的基本思路。然而，由于信息安全的多层次、多因素和动态性等特点，管理手段的应用在一个完整的信息安全防范方案中必不可少。信息安全管理的模型、流程和方法最近几年有了长足的发展。信息安全管理的相关标准、法规也如雨后春笋般相继被推出。信息安全管理作为战略、信息安全技术作为手段，“三分技术、七分管理”的理念正在为社会各界广泛接受。

网络空间安全系列教材是我们专为信息安全教学和科研推出的一款系列书籍，内容涵盖网络空间安全领域的方方面面。系列教材既可作为高等院校网络空间安全及相关专业研究生和高年级本科生的教材使用，也可以作为相关专业人员全面参考的系列手册。

作为网络空间安全系列教材之一，本书在汇总作者及所在团队多年来信息安全管理相关工作的基础上，还提炼了国内和国际上信息安全管理的最新成果。本书在保证知识点精炼的基础上，全面吸纳了最新国内外信息安全管理相关标准和指南的内容，能够反映出信息安全管理理论与方法的研究和应用现状。本书第 1 章概述了信息安全、信息安全管理的概念，信息安全管理的基本原则，以及国内外的研究发展情况；第 2 章详细介绍了国内外的信息安全管理相关标准与法律法规；第 3 章介绍了信息安全管理体系（ISMS）；第 4 章介绍了信息安全风险评估的原则与方法；第 5 章介绍信息系统安全测评的关键内容；第 6 章介绍了业务连续性与灾难恢复；第 7 章介绍了信息系统安全审计的原则、体系、流程等；第 8 章介绍了网络及系统安全保障机制相关内容。

本书由河南理工大学计算机科学与技术学院牵头，与电子科技大学合作编写。参加本书编写工作的有：汤永利、陈爱国、叶青、闫玺玺。具体编写分工如下：闫玺玺编写第 1～2 章，汤永利编写第 3～4 章，叶青编写第 5 章，陈爱国编写第 6～8 章。高玉龙、张亚萍、赵翠萍等几位研究生参与了本书部分章节的资料收集和整理，诚挚感谢他们对本书所做的贡献。

本书在编写过程中，除引用了作者自身的研究内容和成果外，还大量参考了众多国外优秀论文、书籍以及在互联网上公布的相关资料，我们尽量在书后面的参考文献中列出，但由于互联网上资料数量众多，出处杂乱，可能无法将所有文献一一注明出处。我们对这些资料的作者表示由衷的感谢，同时声明，原文版权属于原作者。

本书作为教材，教师在讲授时可以根据学时做出一些取舍。本书全部讲授建议 36 学时，如有更多学时安排，建议酌情增加信息安全管理实践方面的内容，以深化对全书内容的理解。

信息安全管理是信息安全领域中的新的分支，代表了信息安全发展的一种趋势，本书尝试对此领域的理论和方法做一些归纳，以期有益于读者。

由于作者的水平有限，书中难免有一些缺点和错误，真诚希望读者不吝赐教。

编著者

目录

第 1 章 绪 论

信息技术创立、应用和普及是 20 世纪技术革新最伟大的创举之一，借此，人类正在进入信息化社会，人们对信息、信息技术的依赖程度越来越高。与此同时，信息安全问题日渐突出，情况也越来越复杂。

信息安全管理是保障信息系统安全的有力手段，是当今世界各国都在努力推广与应用的重点课题。它涉及的内容广泛，包括技术、方法、保障体系等多方面内容。本章主要阐述信息安全的概念、信息安全管理的概念、信息安全管理的指导原则、信息安全管理的意义、信息安全管理的国内外研究发展，并对本书内容安排进行了说明。

1.1 信息安全

1.1.1 信息安全的现状

由于信息具有易传输、易扩散、易破损的特点，信息资产比传统资产更加脆弱，更易受到损害，信息及信息系统需要严格管理和妥善保护。

1988 年 11 月 2 日，康奈尔大学的研究生罗伯特·莫里斯（22 岁）设计了第一个蠕虫程序，设计初始目的是验证网络中自动传播程序的可行性。该程序感染了 6000 台计算机，使互联网不能正常运行，造成的经济损失达 1 亿美元。程序只有 99 行，利用了 UNIX 系统中的缺点，用 Finger 命令查联机用户名单，然后破译用户口令，用 Mail 系统复制、传播本身的源程序，再编译生成代码。莫里斯因此被判 3 年缓刑、罚款 1 万美元、做 400 小时的社区服务。

1998 年 6 月 2 日，首次出现 CIH 的报道。CIH 病毒是由中国台湾大学生陈盈豪编制的，其动机是“为自己设计病毒”。CIH 病毒 1998 年 4 月 26 日发作，可导致主板、硬盘损坏，变种版本极多，危害严重。1999 年 4 月 26 日 CIH 1.2 版本首次大范围爆发全球超过 6000 万台计算机遭到不同程度破坏；2000 年 4 月 26 日 CIH 1.2 版本第二次大范围爆发，全球损失超过 10 亿美元；2001 年 4 月 26 日 CIH 第三次大范围爆发，仅北京就有超过 6000 台计算机遭 CIH 破坏，瑞星修复硬盘数量当天接近 400 块。

2000 年 5 月 4 日，“爱虫（LOVE BUG）”病毒大爆发。主要表现是邮件群发、修改文件、消耗网络资源。“爱虫”大爆发两天之后，全球约有 4500 万台计算机被感染，造成的损失已经达到 26 亿美元。此后几天里，“爱虫”病毒所造成的损失还将以每天 10 亿～15 亿美元的速度增加。

近两年也发生了几起重大的信息安全事件，2014 年 1 月 21 日，中国互联网出现大面积 DNS 解析故障。2014 年 10 月 2 日，摩根大通银行承认 7600 万家庭和 700 万小企业的相关信息被泄露。

身在南欧的黑客取得摩根大通数十个服务器的登入权限，偷走银行客户的姓名、住址、电话号码和电邮地址等个人信息，与这些用户相关的内部银行信息也遭到泄露。受影响者人数占美国人口的1/4。2015年4月，超30省市曝安全管理漏洞，数千万社保用户敏感信息或遭泄露。从补天漏洞响应平台获得的数据显示，目前围绕社保系统、户籍查询系统、疾控中心、医院等大量曝出高危漏洞的省市已经超过30个，仅社保类信息安全漏洞统计就达到5279.4万条，涉及人员数量达数千万，其中包括个人身份证、社保参保信息、财务、薪酬、房屋等敏感信息。

不断发生的信息安全事件，对信息安全提出了严峻的挑战。据统计，全球平均20s就发生一次计算机病毒的入侵；互联网上的防火墙大约25%被攻破；窃取商业信息的事件平均以每月260%的速度增加；约70%的网络主管报告因机密信息泄露而受到损失。国家与国家之间的信息战问题更是关系到国家的根本安全问题。信息安全已成为信息社会重要的研究课题。

1.1.2 信息安全的概念、特点及意义

1. 信息安全的概念

关于信息安全，不同组织有不同的定义，国际标准化组织对信息安全的定义是："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到破坏、更改和泄露"。在我们常见的很多信息安全文献中定义信息安全主要包括3个方面：机密性、完整性、可用性。目前，信息安全的内涵已从传统的机密性、完整性和可用性3个方面扩展到机密性、完整性、可用性、真实性、抗抵赖性、可靠性、可控性等更多领域。各信息安全属性的含义如下。

（1）机密性：信息不泄漏给非授权的用户、实体或者过程的特性。

（2）完整性：数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

（3）可用性：可被授权实体访问并按需求使用的特性，即当需要时应能存取所需的信息。

（4）真实性：信息所反映内容与客观事实是否一致的特性。

（5）抗抵赖性：证实行为或事件已经发生的特性，以保证事件或行为不能被抵赖。

（6）可靠性：保持持续的预期行为及结果的特性。

（7）可控性：对信息的传播及内容具有控制能力，访问控制即属于可控性。

2. 信息安全的特点

信息安全在技术发展和应用过程中，表现出以下重要特点。

（1）必然性。当今的信息系统日益复杂，其中必然存在系统设计、实现、内部控制等方面的弱点。如果不采取适当的措施应对系统运行环境中的安全威胁，信息资产就可能会遭受巨大的损失甚至威胁到国家安全。所以，信息安全已引起许多国家、特别是发达国家的高度重视，他们在这个领域投入了大量的人力、物力、财力，以期提高本国的信息安全水平。

（2）配角特性。信息安全建设在信息系统建设中角色应该是陪衬，安全不是最终目的，得到安全可靠的应用和服务才是安全建设的最终目的。不能为了安全而安全，安全的应用是先导。

（3）动态性。信息安全威胁会随着技术的发展、周边应用场景的变化等因素而发生变化，新的安全威胁总会不断出现。所以，信息安全建设是一个动态的过程，不能指望一项技术、一款产品或一个方案就能一劳永逸地解决组织的安全问题，信息安全是一个动态、持续的过程，必须能根据风险变化及时调整安全策略。一成不变的静态策略，在信息系统的脆弱性，以及威胁技术发生变化时将变得毫无安全作用，因此安全策略，以及实现安全策略的安全技术和安全服务，应具有"风险监测—实时响应—策略调整—风险降低"的良性循环能力。

3. 信息安全的意义

信息时代，信息安全不仅关系信息自身的安全，更是对国家安全具有重大战略价值。

（1）信息安全的政治意义。

首先，在任何国家，信息安全都是国家安全战略的重要组成部分，尤其是信息技术的发展及信息战的广泛应用，信息安全作为夺取战略制高点的关键因素越来越被各国政府重视。

其次，在全球一体化的今天，常规的战争形态已经慢慢退出历史舞台，国与国之间的战争形式表现在更早获取和掌握对方的各方面情报信息，进行多种形式的打击（如网络战、电子战、经济战、舆论战等），这都是为了获取对本国的最大经济利益和政治利益。而在这个过程中，信息安全被赋予了格外的关注。

（2）信息安全的经济意义。

经济安全的实质是一国最为根本的经济利益不受侵害，通常一国的经济安全取决于该国产业的竞争能力。信息或信息化对于我国产业竞争能力的提升具有战略价值。这不仅在于信息产业已成为支柱产业，更在于信息或信息化已经成为产业总体竞争力提升的基础性手段和核心标志。农业竞争力的提升对信息化的依赖突出体现在，包括物质装备、种植技术、经营管理、资源环境、农民素质等的现代化，只有依托信息化才能真正实现。工业或工业企业，要在激烈的战争中立于不败之地，必须从整体上实现信息化。

由于信息技术的开放性与经济主体利益的冲突性并存，现实的信息系统同样存在着安全风险。信息或信息化有可能对我国的经济安全水平造成严重的冲击，蕴藏着巨大的风险。确保信息安全有助于规避经济安全风险或最大限度地减少这类风险。

（3）信息安全与社会稳定的意义。

当前，我国正处在全面建设小康社会、构建社会主义和谐社会的重要阶段。改革开放30多年来，我国的综合国力显著增强，经济稳步增长，社会政治稳定，人民安居乐业，为推动科学发展、促进社会和谐营造出良好的社会环境。但也要清醒地看到，天下并不太平，危害社会稳定、国家安全和社会公共秩序的煽动性信息大量存在。

信息的泄露所带来的已不仅仅是经济上的损失，在一些地方，侵害公民个人信息犯罪与绑架、敲诈勒索、暴力追债等黑恶犯罪合流。维护信息安全对于保护公民安全、维护法律尊严和社会稳定，都具有重要意义。

1.1.3 信息安全威胁

信息化进程在加快，信息化的覆盖面在扩大，信息安全问题也就随之日益增多和复杂，其造成的影响和后果也会不断扩大和更趋严重。信息安全面临的威胁主要来自以下3个方面。

1. 日益严重的计算机病毒

计算机病毒本身是一种程序，通过信息流动感染计算机的操作系统，最终目的是侵入对方的信息系统，窃取相关的信息资料。其主要特征有以下几个。

第一，破坏性强。计算机病毒可以造成操作系统和应用系统的瘫痪并破坏侵入对象的信息资源，因此具有很强的破坏性。通过感染计算机的硬盘，可能造成分区中的某些区域上内容的损坏，使计算机瘫痪，无法正常工作。

第二，传播性强。计算机病毒通过网络和信息手段进行传播，其传播瞬间可达，扩散迅速。

第三，扩散面广。由于信息技术的巨大覆盖性和扩散性，通过网络传播能够在很短的时间内扩散到网络节点的其他计算机，而一旦网络服务器被感染，其扩散面将更加广泛，清除病毒所需的时间将是单机的几十倍以上。

伴随着计算机技术的提高，近年来计算机病毒也越来越强大，蠕虫病毒具有很快的传播速度和很强大的破坏力，木马病毒能够对受感染计算机实施远程控制并盗取重要信息，虽然现有的杀毒软件能够查杀一部分病毒，但是不断产生的新型病毒还是能够绕过很多杀毒软件的查杀，对目标对象实施感染。同时，计算机病毒还成为交易商品可以进行网上买卖且呈现公开化的趋势。可以说，日益严重的计算机病毒已经对网络信息安全造成了巨大的威胁。以“震荡波”病毒为例，“震荡波”（Sasser）病毒利用微软公布的 LSASS 漏洞进行传播，通过 Windows 2000/XP 等操作系统，开启上百个线程去攻击其他网上的用户，造成机器运行缓慢、网络堵塞。由于其隐蔽性，在一周之内就感染了全球 1800 多万台计算机。“震荡波”病毒在全球带来的损失超过 5 亿美元。根据有关统计数据显示，“震荡波”造成 73%的中毒计算机不得不申请专业防毒公司解救，63%的中毒者工作受到严重影响，30%的人至少花费 10 小时去除病毒，同时估计全球范围为处理“震荡波”病毒造成的计算机损害要花 9.97 亿美元。

利用病毒、木马技术传播垃圾邮件和进行网络攻击、破坏的事件呈上升趋势。计算机病毒主要为获取受感染者的密码和账号信息，从中获取利益。计算机病毒的入侵主要为盗取用户敏感信息，特别是涉及账号、密码等重要经济信息成为网络非法入侵的主要目标。

2．人为的因素

相对物理实体和硬件系统及自然灾害而言，精心设计的人为攻击威胁最大。人的因素最为复杂，思想最为活跃，不能用静止的方法和法律、法规加以防护，这是信息安全所面临的最大威胁。

人为因素分为两种情况：第一种为用户自己的无意操作失误而引发的网络安全，如管理员安全管理不当造成安全漏洞，用户安全意识淡薄，将自己的账户随意转借他人或与别人共享等；第二种为人为的恶意破坏，人为恶意攻击可以分为主动攻击和被动攻击。主动攻击的目的在于篡改系统中信息的内容，以各种方式破坏信息的有效性和完整性。被动攻击的目的是在不影响网络正常使用的情况下，进行信息的截获和窃取。总之，不管是主动攻击还是被动攻击，都给信息安全带来巨大损失。攻击者常用的攻击手段有木马、黑客后门、网页脚本、垃圾邮件等。

网络黑客（Hacker）是专业进行网络计算机入侵的人员，通过入侵计算机网络窃取机密数据和盗用特权，或进行文件破坏，或使系统功能得不到充分发挥直至瘫痪。从世界范围看，黑客的攻击手段在不断地更新，几乎每天都有不同系统安全问题出现。黑客就是利用网络安全的漏洞，尝试侵入其聚焦目标的。随着计算机和网络技术的普及，世界范围内的黑客数量日益庞大，黑客的对象也越来越趋向难度更高的政府、情报部门、大型企业、银行等网站。同时，黑客之间也出现了协同作战的现象，黑客群体呈现集团化、组织化、政治化，甚至国家行为化的趋势。黑客攻击往往呈现较高的智能性和很强的隐蔽性等特点。从智能性上看，黑客普遍具有相当高水平的计算机操作技术，能够绕过所侵入系统的防火墙和拦截软件；从隐蔽性上看，黑客利用计算机作为窃取信息的载体，并以计算机作为入侵的目标，通过编辑程序达到入侵目的，而非直接入侵所要侵入的地点。黑客的行为虽然一般比较隐蔽，但造成的危害一般比较巨大。从我国的实际情况来看，除传统领域的信息安全受到危害外，更为隐蔽和难以追查的信息安全非法手段是通过一些非政府组织、极端宗教组织等进行的信息安全违法行为，这些行为往往具有手段隐蔽、技术手段高等特点，因此在追查方面也更加具有难度，同时在破坏程度上也更加严重。

3．信息安全管理自身的不足

面对复杂、严峻的信息安全管理形势，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，谋求构建立体的、全面的信息安全管理体系，已逐渐成为共识。与反恐、环保、粮食安全等安全问题一样，信息安全也呈现出全球性、突发性、扩散性等特点。信息及网络技术的全球性、互联性、信息资源和数据共享性等，又使其本身极易受到攻击，攻击的不可预测性、危害的连锁扩散性大大增强了信息安全问题造成的危害。信息安全管理已经被越来越多的国家所重视。