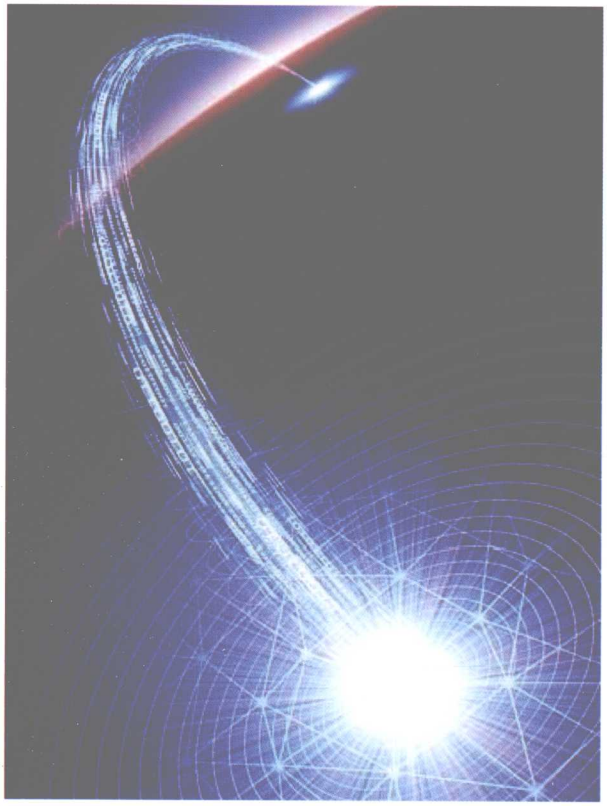
高等学校计算机应用规划教材

信息与网络安全概论
(第三版)

- 信息与网络安全简介
- 信息中心管理与实体安全
- 用户身份验证
- 操作系统安全
- 秘密密钥密码系统
- 新一代密码系统
- 公开密钥密码系统
- 信息验证
- 密钥管理及认证中心
- 多媒体安全
- 网络通信协议安全
- 网络安全
- 移动通信与无线网络安全
- 电子商务安全
- 数据库安全
- 信息安全管理



黄明祥 林咏章 编著

Mc Graw Hill Education

清华大学出版社

高等学校计算机应用规划教材

信息与网络安全概论

(第三版)

黄明祥　林咏章　编著

清华大学出版社

北　京

内 容 简 介

本书系统介绍了信息与网络安全管理各方面的知识。全书共分16章，内容包括信息安全的基本概念以及计算机操作系统的安全，使用密码学处理数据安全，各种信息应用的安全，包括多媒体安全、网络安全、TCP/IP 网络通信协议安全、电子商务安全、数据库安全以及发生安全事件时的应对措施。此外，本书每一章都附带思考练习题，以帮助读者巩固每章所学内容。

本书适合作为高等院校、职业学校的计算机相关专业及信息管理相关专业的“信息与网络安全”、“网络安全”、“信息安全”、“密码学与信息安全”、“电子商务”等课程的教材。由于本书以完全不懂信息安全的初学者为对象，因而也可供各类网络爱好者、企业 IT 经理、网络管理员以及网络安全工程师自学选用。

黄明祥，林咏章
资讯与网路安全概论，第3版

北京市版权局著作权合同登记号 图字：01-2009-3875

图书在版编目(CIP)数据

信息与网络安全概论(第三版)/黄明祥，林咏章 编著. —北京：清华大学出版社，2010.1
(高等学校计算机应用规划教材)
ISBN 978-7-302-21524-0
Ⅰ. ①信… Ⅱ. ①黄… ②林… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08
中国版本图书馆 CIP 数据核字(2009)第 215721 号

责任编辑：王 军 李维杰
装帧设计：孔祥丰
责任校对：胡雁翎
责任印制：王秀菊
出版发行：清华大学出版社 **地 址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn **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
印 刷 者：北京市世界知识印刷厂
装 订 者：三河市溧源装订厂
经 销：全国新华书店
开 本：185×260 **印 张**：22.25 **字 数**：555 千字
版 次：2010 年 1 月第 1 版 **印 次**：2010 年 1 月第1 次印刷
印 数：1～4000
定 价：35.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：(010)62770177 转 3103 产品编号：025686-01

第三版序

随着高速网络技术的提升，各类人群使用计算机来传递、访问及处理信息已经是必然趋势，但是如何使网络中传递的以及存储在计算机系统中的机密数据免遭未经授权人员的窃取、篡改、伪造、破坏等，则是信息时代的当务之急。

信息与网络安全的重要性是编写本书的动机。目前虽然有许多信息与网络安全方面的教材，但内容不是过于理论化，就是过于深奥难懂。本书的目标是希望达到易读、易学、易懂以及内容广泛，尽可能介绍所有有关信息与网络安全的主题，让初学者对这些方面有一定的认识和了解。

本书将信息管理系统中有关信息安全的议题，从环境观点、用户观点、系统观点、数据观点、管理者观点以及法律观点 6 个不同层次来考虑信息安全架构，范围包括实体安全、用户识别、访问控制、密码学、管理控制以及法律制裁 6 大主题。

全书共分 16 章，第 1~4 章介绍信息安全的基本概念以及计算机操作系统的安全；第 5~9 章介绍密码学，主要针对数据安全的处理；第 10~15 章介绍各种信息应用的安全，包括多媒体安全、网络安全、TCP/IP 网络通信协议安全、电子商务安全以及数据库安全；由于不可能有 100%的安全，因此第 16 章介绍了发生安全事件时的应对措施，同时介绍了信息安全管理标准(BS7799)。

本书具有以下特点：

- 尽可能包含信息安全与网络安全的所有相关内容。
- 每章都附有信息安全方面的思考练习。
- 文字力求浅显易懂。
- 尽量举例说明各个议题。
- 提供 PPT 格式的电子教案。

作　者

2009 年 5 月

目　录

第1章　信息与网络安全简介

本章导读

随着信息技术的蓬勃发展、网络应用的日渐普及，计算机及网络技术已广泛地应用在日常生活中，不仅企业利用计算机网络来改善工作效率、扩大电子商务的服务层面以提升竞争力，个人也利用计算机网络来传递邮件、进行数据检索、网上购物、网上竞标及视频点播等服务。信息技术不但为人类带来便利的生活，也颠覆了企业的传统思维，更带动了电子商务的蓬勃发展。人们在享受这些技术带来的便利之余，却常常忽略了这些技术背后所潜在的安全问题。一旦安全方面出现了问题，往往会给企业和个人造成莫大的损失及不便。因此，在发展管理信息系统及电子商务系统的同时，必须先做好计算机系统与网络的安全保护工作。

网络对生活的影响程度与日俱增，黑客利用网络从事计算机犯罪的情况也屡见不鲜。这些计算机犯罪可能牵涉到交易与商务机密，也可能利用这个公用渠道进行其他计算机犯罪行为。例如在网络上贩卖军火、毒品及进行其他非法交易，品行不良的员工泄露组织的机密文件数据以获取利益等，都是现今计算机世界的真实写照。

随着高速网络技术的不断发展，企业与个人利用计算机来传递、访问及处理信息已成趋势。但是，如何保护在网络中传递以及存储在计算机系统中的机密数据，使其免受未经授权人员的窃取、篡改、伪造及破坏等违法行为的威胁，则是信息时代的当务之急。

机密数据相当重要，若不加以有效保护，可能会危及个人权益、公司竞争力，乃至危害国家安全。例如，医院病历数据若遭破坏或篡改，可能导致医疗判断错误；军事信息若遭泄漏或篡改，将极大地影响国家安全。信息安全的重要性由此可见一斑。

信息安全通常注重3类数据：一是机密数据(Confidential Data)、二是敏感数据(Sensitive Data)，三是完整数据(Integrity Data)。机密及敏感数据只允许经过授权的人访问，而禁止未经授权者访问或阅读。机密数据一般是指军事、情报以及有关国家安全的数据统称，而敏感数据则是指政府、机构、企业等具备敏感性的数据。完整数据则是保护该数据的正确性及有效性，禁止该数据被破坏、伪造以及篡改。若无特别指定，本书将以机密数据统称上述3类数据。

1.1　信息安全的威胁

自从美国康奈尔大学学生于1988年散播网络蠕虫(Network Worm)，造成互联网中接近6000台计算机系统死机，计算机用户才开始警觉到信息安全的问题。此后，各种信息安全事件层出不穷，下面列出一些较为重要的真实案例：

- 1994年，一位俄罗斯计算机专家利用网络进入美国花旗银行自动转账计算机系统，窃取1000多万美元的客户存款，并且转存到国外的账户。

- 1996 年，某家知名公司遭到离职员工网络入侵篡改其积体电路布局数据，导致生产出错误晶片，除了增加生产成本，也延误了交货时间，影响了企业的信誉。
- 2000年8月，黑客陆续攻击Yahoo!及其他知名网站(包括Buy.com、eBay.com、Amazon.com 和 CNN.com 等网站)，使这些网站不能提供正常服务，这种攻击称为拒绝服务(Denial of Service，DoS)，从而 DoS 问题开始成为网络安全专家关注的问题。
- 2001 年 3 月，亚马逊网络书店旗下的网站遭到入侵，被窃取近 10 万笔顾客信用卡数据。同年 9 月，Nimda 病毒肆虐全球计算机，使 200 万台计算机瘫痪，全球经济损失估计约 5 亿美元，其他无形的损失则难以计算。

以上只是少数被媒体报道的案例，为了避免影响企业形象，实际上还有更多的案例未被报导。信息安全的目的是为了保护所有信息系统内的资源，包括：

1) 防止未经授权者得到有价值的信息。

2) 防止未经授权者偷窃或复制软件。

3) 避免计算机资源(例如打印机、内存等)被盗用。

4) 避免计算机设备受到灾害的侵袭。

所有影响信息安全并导致系统不能妥善保护资源的因素都属于信息安全的威胁，必须加以防范。一般将信息安全的威胁分为以下几类。

1) 天然或人为

天然的安全威胁起因于自然灾害，导致信息本身或访问渠道遭到破坏。一般常见的灾害有飓风、地震、水灾及火灾等，这些都会对信息系统造成直接的破坏。在传输数据的过程中，可能因为打雷、闪电而造成传输时的干扰与数据改变等问题。其他灾害造成数据的破坏程度不一，例如 2001 年初，某科学园区的大火，导致多数厂商的数据遭受破坏或毁损；同年 9 月，因台风所带来的暴雨侵袭，积水严重，造成许多地下机房的主机设备毁损，存储在设备内的重要数据都受到破坏。

人为的安全威胁是指起因于人为的因素而导致系统的安全受到威胁及攻击。例如，管理人员的疏失或是其他人的蓄意破坏。

2) 蓄意或无意

蓄意的安全威胁是指黑客企图破解信息系统的安全，其目的是想从中获取不当的利益。黑客们利用手中掌握的专业知识不断向计算机系统上的安全漏洞进行探测。有些人是为了测验本身的入侵水平，后来才转为非法盗取计算机资源，从而触犯法律；而有些人则一开始就以盗窃或破坏重要机密数据为其目的。

在信息安全的威胁中，最不易防范的就是蓄意的安全威胁。由于牵涉到人的因素，蓄意安全威胁的可变性很强，再精良的计算机设备也无法预估攻击者的思考模式与行为，因此这方面的安全威胁是最难以克服的。在这种破坏中，包含了许多为目前大多数人所熟知的破坏行为，如计算机病毒、黑客攻击及其他计算机犯罪等。

无意的安全威胁则是由于系统管理不良或系统管理员的疏忽，导致系统出现安全上的漏洞。例如，架设电子商务网站时，为了使外界的用户可以浏览网页，而把网页文件权限设置为只读。如果系统管理员不小心将目录或文件的权限设置成所有人都可以读写，那么此网站

将很容易被入侵。又如，架设 NT 服务器(Server)或 MS SQL 服务器时，很多系统管理员会忘记更改预设的超级用户的密码(注意，NT 及 MS SQL 的超级用户 ID 及密码均为 Administrator)，这使得黑客可以很轻易地取得系统的控制权。许多安全问题是在正常的操作行为下无意间发生的，并可能危及系统安全，大部分原因是由于用户的训练不足及疏忽所引起的。

3) 主动或被动

黑客攻击又可分为主动攻击与被动攻击。在双方传输信息的过程中，窃取信息或是在他人的计算机中植入木马程序，直接取得计算机中的资源及机密文件，并不让传输者发觉，这样的行为均属于被动式的攻击。而主动攻击则是指利用大量封包传送，使受害者的计算机、服务器瘫痪；或是篡改传送中的封包数据；又或是传送假的信息给另一个具有利益关系的受害者，造成其财务上或精神上的损失。被动的安全威胁行为并不会更改信息系统的数据，黑客的主要目的是窥探机密数据，以获取不当利益或仅是探取他人隐私。相反的，主动的安全威胁行为则会篡改或者破坏信息系统的数据，从而以假数据欺骗用户，或者让用户不能正常得到数据或得到篡改过的数据。主动或被动的安全威胁将在本书第 12.1 节介绍网络安全威胁时再进一步说明。

4) 实体或逻辑

实体的安全威胁，其对象为实际存在的硬件设备。逻辑的安全威胁，其对象则为信息系统上的数据。典型的实体安全威胁是歹徒直接侵入计算机机房，用铁锤或其他方式破坏计算机设备，使其不能正常运转。本书第 2 章将介绍实体安全，以避免这种类型的安全威胁。

另外，计算机硬件经过长期运算、使用，会造成硬件物理性的弹性疲劳或损坏。若无适当的保养，很容易导致其运算错误，造成决策失误。软件所产生的错误可以从模拟结果得知，但硬件产生的问题则不易被侦测出来。其他存储硬件损毁则会发生重要数据遗失等问题。如果关键性硬件设备发生损坏(如军事上的飞弹导航系统)，所造成的损失要远比没有使用信息技术大得多。因此，平常做好保养以及确保硬件安全，是系统管理员必须要重视的问题。

1.2　信息安全的基本要求

由于网络的便捷性及多功能性，不论是企业还是政府部门，对信息安全的需求都将随着网络的快速发展日益加大。对重要的信息内容加强其安全性，以符合不断变化的环境。但是，所谓“道高一尺，魔高一丈”，对于信息安全而言，威胁时刻存在，一项防护总是会面对另一种威胁，从而呈现出一场安全与威胁的拉锯战，互相制衡。以下针对安全上的需求与威胁进行简单介绍。

信息安全的目的即在于防止影响信息安全的威胁。基本上，一套优秀的安全信息系统需要具备下列 7 个特性：保密性、完整性、验证性、可用性、不可否认性、访问控制以及审核。

1) 保密性或机密性(Confidentiality)

确保信息的机密，防止机密信息泄漏给未经授权的用户。机密性数据内容不能被未经授权者所窃取，而仅能被授权者所访问。这里所谓的访问包括浏览及打印。另外，数据是否存在于系统中也是一项很重要信息，必须加以保密，不能直接或间接被不法人士所了解。

一旦数据经过传递的操作，就会存在信息内容被窃取的风险，尤其是组织的决策文件、职员工资或国家机密数据等，对于保密性的需求非常重要。此项需求主要是确保数据信息不会遭受到第三者偷窥或窃取。

为确保数据传输的隐私，可通过数据加密程序以达到此目标。如果国防机密政策或者企业中的营销策略等未考虑到此需求，忽略此需求的重要性，则都将可能造成极为严重的后果。国家安全遭受威胁，人民生活将陷入恐慌：而企业营销将可能受到同行阻碍，或是对手利用窃取所得的信息，率先抢占市场。因此，通过对数据隐私的保护，可以避免上述问题的产生，数据保密性为信息安全的主要要求之一。

2) 完整性(Integrity)

数据内容仅能被合法授权者所更改，不能被未经授权者所篡改或伪造。这里所指的“更改”包括创建(Creating)、更改(Changing)、更新(Updating)及删除(Deleting)等。数据完整性必须要确保数据传输时不会遭受篡改，以保证数据内容的完整性。

在系统设计、分析及规划时，必须考虑到数据输入错误、用户使用不当或蓄意破坏数据、传送失败及系统处理错误的可能性，从而减少数据产生错误的情况发生。因此，系统在设计之初，必须将这些可能的问题一并列入考虑范围，不但要检验数据格式合理及有效，更需要保证数据正确且可用。

另外，第 7 章介绍的“数字签名”可用来确保数据在传输过程中不会被黑客篡改及伪造，从而保证数据的完整性。

3) 验证性(Authentication)

验证性包括身份验证(Entity Authentication)及数据或消息来源验证(Data or Message Authentication)。信息来源的验证是要能确认数据信息的传输来源，以避免有恶意的传送者假冒原始传送者传送不安全的信息内容。一般均利用数字签名或数据加密等方式来解决信息的来源验证问题。

对于用户身份的识别而言，系统必须快速且正确地验证身份。为了预防暴力攻击者(参考第 3.2 节说明)的恶意侵犯，对于用户身份验证的时效性比信息验证要严谨。

根据用户的身份，可以进一步执行访问控制以限制用户的执行权限。为了保护接收者的权益或系统安全，不论是信息还是用户身份的识别，都必须要有很完善的识别机制。

4) 可用性(Availability)

确保信息系统运行过程的正确性，以防止恶意行为导致信息系统毁坏(Destroy)或延迟(Prolong)。另外，数据内容和数据格式均不能被破坏，否则会导致系统不能正常运转，系统必须提供有效及正确的数据给合法用户。这里所谓的“有效数据”必须借助保护控制机制和完整性检查。

5) 不可否认性(Non-Repudiation)

在信息安全需求中，对于传送方或接收方，都不能否认曾进行数据传输、接收和交易等行为，即传送方不得否认曾传送过某份数据，而接收方也无法否认未曾接收到某信息数据。例如，消费者不能否认曾在某个电子商务网站进行交易，商家也不能否认曾收到消费者交易及货款信息。

一般可利用第 7 章所介绍的数字签名及公开密钥基础设施(Public Key Infrastructure，PKI)对用户身份及信息来源做身份验证(User Authentication)及数据来源验证(Message Authentication)，并可再与用户在系统上的活动进行连接，从而实现权责分明及不可否认性。

6) 访问控制(Access Control)

信息系统内每位用户依其服务等级而有不同的使用权限。服务等级越高者其权限越大，相反的，服务等级越小者其权限越小。因此，计算机系统的超级用户(Super User)拥有最高的系统权限，偶尔使用的访客(Guest)权限则是最低，仅能使用简单的基本服务，如使用 BBS 或是浏览产品信息。

访问控制主要是根据系统的授权策略，对用户做授权验证，以确认其是否为合法授权者，防止未经授权者访问计算机系统及网络资源。用户一旦经过身份验证，被确认为本系统的合法用户后，就可以使用本系统所提供的服务或资源。并不是所有合法用户均可以享用系统的所有服务，必须依用户是否被授权而定。例如，张三被授权可以使用打印机，那么张三被确认为合法用户后，就可以使用打印机这种资源。

本书中所说的“合法用户”是指通过身份验证后的用户，而“合法授权者”是指经过系统授权可以访问某些计算机资源的“合法用户”。有关访问控制将在第 4 章介绍。

7) 审核(Audit)

信息系统不可能达到绝对安全，也就是百分之百的安全。任何信息安全产品，其厂商绝对不敢向客户保证安装该产品后客户的系统就可百分之百地高枕无忧，不用再担心黑客入侵。黑客的手法千奇百怪，现在的安全并不意味着明天的安全。因此，必须通过审核记录(Audit Log)来追踪非法用户，一旦发生入侵攻击事件，就可以尽快找到发生事件的原因，以作为恢复系统(Recovery)并预防此类入侵的手法，从而防止系统再一次被入侵。

信息安全必须发展各种保护方法，以满足上述 7 个特性，这些方法将在第 2 章以后陆续介绍。

1.3　信息安全的范围

信息安全的领域相当广泛，所有可确保信息系统正常运行并确保机密数据的保密性及完整性的机制都涵盖在内。一般的管理信息系统(Management Information System，MIS)架构如图 1-1 所示，包含管理信息系统、计算机操作系统以及数据库管理系统。

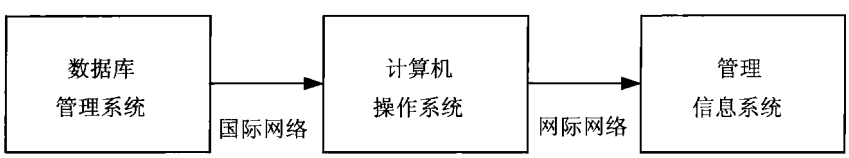


图 1-1　管理信息系统的一般架构

大部分的管理信息系统都会通过数据库管理系统维护数据，早期的管理信息系统与数据库系统处于同一台计算机中，称为单机版信息系统。现在由于机关、企业的规模庞大且分散

各地，信息系统已由原先单机版系统扩展为主从式(Client-Server)或三层式(3-Tier)架构，数据库不需要与管理信息系统在同一台主机。反之，可以分散在不同主机系统上，要访问分散在各地的数据，可通过局域网或网际网络访问。因此，要设计一个安全的管理信息系统，信息安全除了包括数据库安全、操作系统安全及管理信息系统安全之外，还必须涵盖网络安全。

图 1-1 中的管理信息系统可以是会计管理信息系统、人事管理信息系统、财务管理系统、决策支持管理系统以及电子商务系统等。以电子商务系统为例，它牵涉到数据库管理系统、计算机操作系统、电子商务应用系统以及网际网络等。因此，就电子商务系统的安全而言，它的信息安全范围应包含数据库安全、操作系统安全、电子商务安全及网络安全。

数据库安全主要是确保数据库内的数据不被未经授权者所访问或推导出机密数据。计算机操作系统安全包括了访问控制机制及用户验证机制等防护措施。网络安全则泛指信息在公开的网络上传送所需的安全防护。

信息安全的范畴除了包括数据库安全、管理信息系统安全及网络安全外，还必须考虑到整体架构之操作环境的安全问题，包括系统的所有使用人员、操作界面、后端处理程序以及数据库这 4 个模块。

1) 用户

系统的使用者可能是组织中的员工或顾客。若为组织内员工，必须训练其操作系统的能力。若为与系统安全性相关的员工，必须以合同限制其使用各种可能携带的存储设备，例如移动盘、磁盘、光盘等。组织中对外网络与内网络必须有严谨的区分，预防员工将机密信息通过各种方式泄露出去。目前企业或是国营单位都开展安全教育训练，对员工建立道德观，签订合同并制订违约的惩处措施，以确保组织的权益。

2) 操作界面

另一个与用户有着密切关系的系统元素则是用户的操作环境(界面)。若以网络连接后端处理程序，则以网页方式呈现，作为与处理程序连接的前端界面，利用 ASP、JSP、PHP 等网页程序语言产生固定的数据输入格式，并利用各种脚本命令检验输入的数据是否符合所需的数据格式。例如，金额就不能输入文字或身份证格式的数据。对于不同等级的用户，必须要提供不同的页面。例如，通过 ID 与密码(Password)的识别，以确定是管理者还是一般用户，从而给予不同的操作界面，以避免攻击者进入管理界面而拥有更高的权限破坏系统。

3) 后端处理程序

整个系统架构的核心是处理程序，也就是所谓的后端处理程序。它负责处理回应用户所要求的服务，若用户要取得数据库中的数据，也必须通过此系统组件来访问。后端处理程序可以说是系统中的灵魂，因此必须确保来源端的正确性。大部分的做法是规范不同权限的用户，须有不同的处理方式。若为一般用户，不能接触源代码，也没有权限修改程序内容。

4) 数据库

数据库负责保存重要数据与一般数据。依据不同需求，有不同的数据格式与存储方式，若用户要访问数据库中的数据，则可以利用后端处理程序作为桥梁，来得到正确的数据。

1.4　信息系统的安全分析

由于新的攻击方法及安全漏洞不断地被发现，系统管理员很难再根据过去系统运行的经验准则，作为未来系统运行的永久保证，这就增加了建立一个安全的信息系统的难度(注：本书所说的“信息系统”泛指计算机操作系统、数据库管理系统及其他管理信息系统)。因此，构建一个完善的信息系统或电子商务系统必须有下面所述的安全分析及策略方案，以应对突发的安全问题。

1) 弱点分析(Vulnerability Analysis)

对整个系统架构进行了解及测试，系统架设了哪些硬件，例如路由器(Router)、桥接器(Bridge)、网关(Gateway)及防火墙(Firewall)等；使用了哪一种操作系统，例如 Linux、WinNT 及 Novell Network；使用了哪些通信协议，例如 TCP / IP、Ethernet 及 ISDN 等；安装了哪些应用软件，例如 FTP、WWW 及工资管理信息系统等；哪些人会使用本系统，授权了哪些权限给用户等。管理者了解这些信息后，进而分析系统的弱点在哪里，哪些人有可能会来攻击，他们的目的是什么，以及要攻击哪些地方。

此外，目前已有许多系统安全管理工具，系统管理员可以利用这些工具来测试系统是否安全，并测试出系统的弱点所在。利用人工的方法测试网络安全与否，很难完全兼顾各个层面；而使用安全管理工具来帮助测试系统的弱点，可以向管理者提供相关信息，并帮助管理者找出系统最易遭受攻击的地方，进而加强安全防护。

2) 威胁分析(Threat Analysis)

了解系统的弱点之后，接着要分析系统可能会遭受到的安全威胁及攻击。常见的入侵并影响系统安全的方式有利用电子邮件、利用 Telnet 远程登录、发送计算机病毒、试图得到具有高存储权限的账号、删除或移动文件等。系统管理员应随时上网浏览最新的黑客入侵信息，以防止计算机系统与网络安全危机的发生。

3) 对策分析(Countermeasure Analysis)

针对这些弱点及所面临的安全威胁，应制定相应的安全策略及所需的安全机制。例如访问控制、用户认证、加密及数字签名等，这些技术均会在第 2 章以后陆续介绍。此外，还应对其成本效益做分析工作。

4) 风险分析(Risk Analysis)

不仅要定期评估及分析系统的风险，而且对于部分重要数据还必须采取进一步的防御。例如定期做备份及恢复处理等，确保当系统发生安全问题时重要数据不被损坏，从而降低问题发生时所带来的风险及损失。

发生安全漏洞所造成的损失包括有形损失和无形损失两种。有形损失包括硬件及软件设备、人力成本、开支成本及其他因工作延迟所造成的损失。无形损失是指公司形象受到影响，其损失费用则无法计算。通常投资在信息安全方面的费用应小于系统发生安全漏洞后所造成的损失，但要大于其损失的十分之一。例如，若预计某系统一旦发生安全事件所造成的损失为 1000 万元，那么所投资的成本就应该在 100 万到 1000 万元之间。