论电子商务安全管理概论

王　彬

海南科技职业大学　海南海口　571126

摘　要：本文主要论述的是电子商务的安全问题，从电子商务的现状、电子商务面临的安全、电子商务的安全技术、与电子商务安全有关的协议技术阐述了电子商务的安全管理。从而让我们知道安全是电子商务的核心。电子商务对网络安全与商务安全的有着双重要求，使网络安全与商务密不可分。电子商务的发展是最大的应用趋势，是国际经贸全新的超前一种形式，是我国经济生活中的新手段。

关键词：电子商务；安全；管理；问题

电子商务是利用各种电子化进行的商务活动，尤其是互联网，其价值的实现依托于网络里，它已成为互联网应用的一个趋势和金融商贸的传播模式之一。如何建立一个安全的应用环境呢？对我们所提供信息有很多的保护，这已成为电子商务必须面对的一个问题。电子商务的安全管理，就是通过一个完全的综合保障体系，来规避信息风险、信用风险、管理和法律风险，以保证交易的顺利进行。网上交易安全性是电子虚拟市场的首要问题。

电子商务的重要技术特征，是利用网络来进行传输和处理，电子商务的安全主要包括两个方面：商务和网络安全。而这些安全的实现必须需要一些具体的安全技术，遵循安全协议。首先，它是保证游戏规则顺利实施的前提，因为市场竞争是公正、公开、公平，如无法保证市场交易的安全，会导致非法交易，使市场规则无法贯彻执行。其次，它是保证电子交易顺利发展的前提，虽然网上交易可降低交易费用，但网上交易安全性无法得到保证，会造成合法交易双方利益的损失，导致交易双方为规避风险，选择传统的更安全的交易方式，会制约电子虚拟市场的发展。

无论从市场本身发展，还是保护市场交易利益来看，保证网上交易安全，是电子虚拟市场要解决的首要和基本问题，这需要各方配合，加强对网上交易安全的监管。

1 电子商务安全现状

如今电子商务安全的问题比较严重，最突出表现在计算机网络和商业诚信问题上。随着网络技术的广泛应用，电子商务安全日益突出。最近，我国因特网用户激增，至今已超过了 130 万，不少企业更是拥有自己的网站，网络交易热潮也随之而来。因为网络自身的开放性，安全和黑客事件时有发生，据资料，利用计算机网络进行各类违法行为，在中国每年 30%的速度递增。更有媒介报道，中国 95%的与互联网相连的网络中心遭到过黑客的攻击或侵入，安全隐患已经成为电子商务的严重阻碍。

电子商务的安全，可以分成技术安全、管理安全两种类型。技术安全通过各种黑客手段窃取企业相关的机密文件，以及用户的 ID、密码，甚至网络的银行账号、密码等，造成了重大的经济损失。安全管理则是指对参与电子商务过程中的各个环节的人员的管理和预防手段，最终导致电子商务的安全事件。

2 电子商务面临的安全问题

2.1 网络信息安全方面问题

电子商务服务器是核心，安装大量的软件和商家信息，且服务器上的数据库里，有电子商务活动过程中的保密数据。因而服务器容易受到安全的威胁，且一旦出现安全问题，后果也是非常严重。

网络安全指计算机和网络本身存在的安全问题，也就是要保障电子商务平台的安全性和可用性，网络安全出现的问题，一般表现为：

2.1.1 交易信息内容被篡改

从贸易活动角上看，交易信息是商务活动中，进行贸易活动形成的一种信息，包括客户订单信息、订单确认的信息、客户的个人信息等。这些信息有一定机密性，在信息传递的过程中，利用互联网或电话网收到，对这些交易信息进行篡改或截获。非法用户在网络传输上使用的不正当手法，非法拦截会话数据，获得合法用户的有效信息，最终造成合法用户的一些核心业务数据泄密，从而使信息失去了真实性和完整性，导致用户无法正常交易，还有一些非法用户，利用截获的网络数据再次发送，恶意攻击对方网络硬件和软件。

2.1.2 电子支付信息盗取

电子支付是在电子商务活动中进行的支付方式。支付信息包括：客户银行的账户、密码和个人银行识别码的信息。这些信息具有绝对机密性，防止盗用信息，伪造假身份信息进入系统，利用信息进行非法的活动，是电子商务活动中要解决的问题。绝大多数网站采用网络安全设备，耗费巨资，而安全设备本身问题，导致这些设备并未起到应有的作用。很多安全产品对配置人员的技术要求不很高，超出对普通网管的技术要求，厂家在当初给用户做出的正确配置，通过系统改动，需要改动相关的安全设备设置时，很容易出现安全问题。

实施网络安全防范的措施应做到：加强主机的安全，做好安全配置，及时安装安全补丁，减少漏洞；安装防火墙和防病毒软件，加强内部网整体防病毒的措施；使用各种系统漏洞检测软件，定期对网络系统进行分析，找出存在的安全隐患，并进行及时的修补；从路由器到用户各级，要建立完善访问控制措施，安装防火墙，加强授权认证和管理；利用相对数据存储，恢复措施和数据备份；对敏感设备和数据，建立物理逻辑隔离措施；在公共网络上传输敏感信息，要进行高强度的数据加密；建立详细的审计日志，检测入侵攻击。充分利用已公布的计算机安全和交易安全的法规，为电子商务护航。

2.1.3 系统漏洞

互联网的出现，为电脑病毒的传输提供了最好的媒介，不少新病毒通过互联网作为自己的传播途径。电脑病毒问世以来，各种新

型病毒及变种迅速发展，不少新病毒以互联网作为传播途径，仍有众多病毒借助于互联网传播得更快，而在电子商务领域，有效防范病毒是一个十分紧迫的问题。非法者借助电子商务存在的漏洞进入系统，对数据进行篡改，取消用户订单信息，生成虚假信息的方式。电脑使用的是未经过网络安全配置的操作系统，不管什么操作系统，在缺省安装的条件下，都会存在一些安全问题，而将操作系统按照缺省安装后，再配上长密码就认为这是安全的想法，是不可靠的。因计算机本身存在软件的漏洞和“后门”，往往是网络攻击的首选目标。一个全方位计算机网络安全体系结构，通常包含网络的物理安全、访问系统安全、控制安全、用户安全、信息加密、管理安全和安全传输。而这一切的实现依靠各种先进的主机安全技术、访问控制技术、身份认证技术、密码技术、防火墙技术、安全管理技术、安全审计技术、系统漏洞检测技术、黑客跟踪技术等。随着安全的核心系统，VPN 的安全隧道，身份认证及网络底层数据加密和网络入侵主动监测的应用，从多层面加强了计算机网络整体的安全性，在攻击者和受保护者的资源间，建立了多道严密的安全防线，增加了恶意入侵难度。为保证电子商务活动顺利进行，必须有完善的网络体系为其提供稳定，强而有力的支撑。相对而言，袭击者的风险却显得非常小，可以在袭击后很快消失得无影无踪，使对方没有实行报复打击的可能，这使他们的活动更加的猖獗。

2.2 系统安全问题

在电子商务中，网络安全包括以下两个方面：对于企业来说，首先是信息的安全与交易者的安全，但是信息安全前提条件是系统的安全。

系统安全的技术和手段有冗余技术，网络隔离技术，访问控制技术，身份鉴别技术，加密技术，监控审计技术，安全评估技术等。

2.2.1 网络系统

系统安全是网络的开放性、无边界性、自由性造成的，解决的关键是把被保护的网络从开放，无边界，自由的环境中独立出来，使网络成为可以控制、可以管理的内部系统，由于网络是应用系统的基础，网络安全成为首要问题。解决网络安全主要方式：

网络冗余--是解决网络系统单点故障重要措施。对关键性网络线路、设备，通常采用双备份、多备份的方式。网络运行时双方对运营状态，相互实时监控并自动调整，当网络的一点发生故障或网络信息流量突变时，能在有效时间内切换分配，保证网络正常运行。

系统隔离——物理隔离和逻辑隔离，主要从安全等级考虑划分的网络安全边界，使不同级别的网络或信息媒介，不能相互访问，从而达到的安全目的。对业务网络和办公网络采用 VLAN 技术，通信协议等实行逻辑隔离划分不同的应用子网。

访问控制--对网络不同信任域实现双向控制和有限访问原则，使受控子网或主机访问权限、信息流向能得到有效控制。相对网络对象而言，需要解决网络边界的控制和网络内部控制，对网络资源保持有限访问原则，信息流可根据安全需求实现单向或双向控制。访问控制最重要的就是防火墙，一般安置在不同点域的出入口处，对进出网络的 IP 进行过滤，按企业安全政策进行信息流控制，同时实现网络的地址转换、实时信息的审计警告等功能，高级防火墙还实现基于用户的细粒度访问控制。

身份鉴别——对网络访问者权限的识别，通过三种方式验证主体的身份，一是主体的秘密，如用户名、密码；二是携带的物品，如磁卡、IC 卡、动态口令和令牌卡等；三是特征或能力，如指纹、声音、视网膜、签名。加密为了防止网络的窃听、泄漏、篡改和破坏，保证信息的传输安全，对网上数据使用加密手段是最有效的方式。加密可以在三个层次实现，链路层加密、网络层加密、应用层加密。链路加密侧重通信链路，不考虑信源和信宿，对网络高层主体是透明的。网络层加密采用 IPSEC 核心协议，具有加密和认证双重功能，是在 IP 层面实现的安全标准。通过网络加密可以构造企业的虚拟专网，使企业在较少投资下，得到安全较大的回报，并保证用户应用安全。

安全监测--采取信息侦听方式寻找未授权网络访问尝试和违规行为，包括网络系统扫描、预警、阻断、记录、跟踪，发现系统遭受的攻击伤害。网络扫描监测系统，作为对付电脑黑客的最有效的技术手段，具有实时、自适应、主动识别、响应等特征，广泛应用于各行各业。网络扫描针对网络设备的安全漏洞，进行检测和分析，包括网络的通信服务，路由器，防火墙，邮件，WEB 服务器等，识别能被入侵者利用非法的网络漏洞。网络扫描系统将对检测到的漏洞信息形成详细的报告，包括位置、详细描述及建议的改进方案[1]。

2.2.2 操作系统

操作系统负责信息发送，管理，设备存储空间和各种系统资源的调度，作为应用系统的软件平台，具有通用性和易用性，操作系统安全性自接，关系到应用系统安全，操作系统安全可分为应用安全和安全漏洞的扫描。

应用安全--可以杜绝使用来历不明的软件。用户可安装操作系统，保护与恢复软件，并作相应的备份。

系统扫描--通过不同版本的操作系统，进行扫描分析，对扫描漏洞自动修补，形成报告，保护应用程序、使数据免受盗用、破坏。

2.2.3 应用系统

办公系统文件的安全存储：要利用加密手段，配合身份鉴别和密码保护机制 IC 卡、安全 PC 卡等，使存储在本机和网络服务器上的个人和单位重要文件，处于安全存储状态，使他人即使通过各种手段，非法获取相关文件或存储介质磁盘等，也无法获取相关文件的内容。

文件邮件的安全传送：对通过网络传送的文件进行安全处理（加密、签名、完整性的鉴别等），使被传送的文件只有指定的收件者，通过相应的安全鉴别机制 IC 卡、PC 卡才能解密和阅读，杜绝文件在传送或到对方的存储过程中，被截获、篡改等，用于信息网中报表传送、公文卜发等。

2.3 商务安全问题

商务安全是商务交易在网络媒介中，体现出来的安全问题，就是要实现电子商务的保密性、真实性、完整性和不可抵赖性。在电子交易中，曾采用过简单的安全措施。如将网上交易中最关键数据如信用卡号码等用电话告知，以防泄密，网上交易后，再用其他方式做确认，以保证真实性和不可抵赖性。这些方法操作不便，有一定的局限性，不能实现其真正的安全性。

2.3.1 商务安全普遍存在的安全隐患

2.3.1.1 窃取信息

信息在传输过程中，未采用相应的加密措施或者加密强度不够，导致数据信息在网络上以明文的形式传送。入侵者在数据经过

的设备或线路上，采用截获方法截获信息，通过对窃取数据的分析比对，找到信息格式和规律，进而得到了传输信息的内容，导致消费者的消费信息，账号密码和企业的商业机密等信息外泄。

2.3.1.2 篡改信息

当入侵者掌握信息的规律和格式后，通过各种的技术方法和手段，对网络传输中的信息进行截获修改，再发至原先指定目的地，从而破坏信息真实性。入侵者改变信息流的次序，更改信息内容，删除信息某些部分，甚至在信息中插入一些内容，使接收方做出错误判断与决策。

2.3.1.3 信息假冒

由于掌握了数据格式，并篡改通过的信息，攻击者会进一步冒充合法用户，获取和发送信息，而远端接受方或者发送方通常不易分辨。方式有伪造用户和商户的收定货的单据，修改相关程序的使用权限等。

2.3.1.4 信息破坏

由于攻击者的侵入网络，对获得对网络中信息的权限修改，对网络中现有机要信息进行篡改甚至删除，后果是非常严重的。

2.3.2 电子商务交易的要求

2.3.2.1 信息的保密性

交易中的商务信息需要遵循一定保密规则。因为信息往往代表着国家、企业和个人的商业机密。在以往传统的纸面贸易中，采用邮寄封装或通过可靠的通信渠道，传送商业信息，达到保密的目的和要求。而电子商务建立在一个开放的互联网络环境上的，所依托的网络本身就是由于开放式互联形成的市场，赢得了电子商务，因此在这新的支撑环境下，势必要用相应技术和手段，来延续和改进信息的保密性。一般用密码技术来实现[2]。

2.3.2.2 信息的完整性

不可否认，电子商务的出现以计算机代替了大多数复杂的劳动，以信息系统的形式，整合化简了企业贸易中各个环节，但网络的开放和信息的处理自动化，使如何维护贸易各方的商业信息的完整、统一出现了问题。由于数据输入时意外差错（如计算机处理过程中死机，停电等），可导致贸易各方信息不一致。此外，数据传输过程中的信息丢失（如数据包丢失），信息重复或信息传送次序差异（如网络堵塞重发）也会造成贸易各方信息的不同。而贸易各方各类信息的完整性，势必影响了贸易过程中交易和经营策略。因此保持贸易各方信息的完整性，是电子商务必备的基础。完整性一般是通过提取信息摘要的方式来获得。

2.3.2.3 信息不可抵赖性

在交易中出现交易抵赖的现象，如信息发送方在发送操作完成后，否认曾经发送过该信息，或与之相反，接受方收到信息并不承认曾经收到了该条消息。因此确定交易中的任何一方，在交易过程中所收到的信息正是自己的合作对象发出的，而对方也没有被假冒，是电子商务活动顺利进行的保证。信息的保证可通过对发送的消息数字签名来获取。身份确定一般都采用证书机构 CA 证书的方法来实现。在电子商务活动中还有很多要求，相信在电子商务发展中，必将涌现各种技术和各项法律，规范人们的需求，帮助其实现，保证电子商务交易严肃性和公正性。

2.3.3 交易协议的安全性得不到保障

电子商务安全问题仍然是影响发展的主要因素。由于网络技术迅速发展，电子商务引起了广泛注意，在网络上进行商贸活动，如何保证传输数据安全成为电子商务能否普及最重要的因素。交易双方进行的交易内容被第三方窃取，交易一方提供给另外一方使用的证明文件，被第三方非法使用，从而进行商业的欺诈。当攻击者掌握信息的格式和规律后，会通过各种技术手段和方法，将网络传输的信息数据篡改，然后发向目的地，破坏数据真实性和完整性。用户在电子交易过程中的数据，是以数据包形式来传送的，恶意攻击者容易对电子商务网站展开数据包拦截，对数据包进行修改和假冒。TCP/IP 协议就是建立在可信的环境下，缺乏相应安全机制，这种地址的协议本身容易泄露口令，根本没有考虑到安全问题；TCP/IP 协议完全公开的，远程访问的功能使得许多攻击者，无须到现场就能得手，连接的主机基于互相信任的原则，这些性质使网络更加的不安全[3]。

2.3.4 电子商务管理不规范

电子商务的发展也给传统贸易带来了巨大的冲击，带来了经济结构的变革，电子商务也给世界带来了全新的商务规则和销售方式，这要求管理者要做到科学规范。政府应积极介入网络的电子商务管理，促进网络健康稳定发展，制约网络上的违法犯罪行为，电子商务交易平台是非常重要的，是电子商务的门面，内部的经营管理体系则是完成电子商务活动必备条件，它关系了业务最终能不能实现。

2.3.5 交易身份的不确定

电子商务，是一种全球各地广泛的商业贸易活动。在开放的网络环境下，基于浏览器/服务器的应用方式，在买卖双方都不谋面的情况下，进行各种商贸活动，实现消费者网上购物、商户之间网上交易和在线电子支付等各种商务活动，交易活动，金融活动，相关的综合服务活动。正是基于这个特点，攻击者会通过非法的手段，盗窃合法用户的身份信息，仿冒合法用户身份与他人进行交易。

3 电子商务的安全技术

信息安全技术，在电子商务系统中作用非常重要，它守护商家和客户的重要机密，维护商务系统的信誉和财产，同时为交易双方提供极大的方便。因此，只有采取了必要和恰当的技术手段，才能提高电子商务系统的可用性和推广性。电子商务系统使用的安全技术，包括网络安全技术，加密技术，数字签名，密码管理技术，认证技术，防火墙技术以及相关一些安全协议标准等[4]。

3.1 加密技术

加密技术是保障电子商务安全的重要手段，为保证电子商务安全，使用加密技术对敏感信息进行加密，保证电子商务保密性、完整性、真实性和非否认服务。如同很多 IT 技术一样，加密技术也层出不穷，为人们提供很多的选择余地，但与此同时带来了一个严重问题——兼容性，不同企业可能会采用各自不同标准。加密技术向来由国家控制的，如 SSL 的出口受到美国国家安全局的限制。目前，美国的企业一般都使用 128 位的 SSL，但美国只允许加密密码为 40 位以下的算法出口。虽然 40 位的 SSL 具有一定的加密强度，但其安全系数显然比 128 位的 SSL 要低很多。美国以外的国家，很难真正在电子商务活动中充分利用 SSL，这不能不说是一个遗憾。目前，我国由上海电子商务安全证书管理中心推出了 128 位 SSL 算法，弥补了国内的这空缺，为我国电子商务安全带来了广阔前景。

3.1.1 常用的加密技术

对称加密/对称密码加密/专用密码加密，该方法对信息加密和解密都使用了相同的密码。使用对称加密方法会简化加密的处理，每个贸易方都不需彼此研究和交换专用的加密算法，而是采用相同加密算法并只交换共享专用密码。

非对称加密/公开密码加密，在这种加密体系中，密码被分解为一对。这对密码中的任何一方都可作为公开密码，通过非保密方式向他人公开，而另一方则作为专用密码保存。公开密码用于对机密的加密，专用密码则用于对加密信息解密。专用密码只能由生成密码对贸易方掌握，公开密码可以广泛发布，但它只对应生成该密码的贸易方[5]。

3.1.2 数字摘要技术

该方法也称安全 Hash 编码法或 MD5。该编码法是采用单向 Hash 函数，将需加密的明文“摘要”成一串 128bit 密文，这一串密文称为数字指纹，具有固定长度，并且不同明文摘要其密文结果是不一样，而同样明文其摘要保持一致。数字签名：数字的签名是将数字摘要，公用密码的算法两种加密方法同时使用。它的主要方式是报文发送方从报文的文本中生成一个 128 位的散列值。采用单向 Hash 函数可以将需加密的明文“摘要”成一串 128bit 密文，即数字指纹，它有固定长度，且不同明文摘要成密文，其结果总是不同，而同样明文其摘要必定一致。这摘要便成为验证明文是否是“真身” “指纹”了。发送方用自己专用密码对这个散列值进行的加密来形成发送方数字签名，然后这个数字的签名将作为报文附件和报文一起发送报文的接收方。报文接收方首先从接收到原始报文中计算出 128 位散列值（或报文摘要），接着再用发送方公开密码来对报文附加数字签名进行解密。如果两个的散列值相同，那接收方就可确认该数字签名是发送方的。通过数字的签名能够实现对原始报文鉴别和不可抵赖性，有效防止了签名否认和非正当签名者假冒。数字时间戳：是对交易文件时间信息所采取安全措施。该网上安全的服务项目，由专门机构提供。时间戳是一个经加密后形成凭证文档，它包括需加时间戳文件的摘要，数字时间戳的服务收到文件日期和时间，数字时间戳服务数字签名。数字证书：数字证书称为数字凭证，是用电子手段证实一个用户身份和对网络资源的访问权限，有个人凭证，企业（服务器）凭证，软件（开发者）凭证等三种。

3.1.3 数字签名

信息是由签名者发送；信息在传输的过程中未曾作过任何修改。这样数字的签名就可用来防止电子信息被修改而有人作伪；或冒用别人名义发送的信息；或发出（收到）信件后又加以否认的情况发生。

3.1.4 数字时间戳

它是一个经加密后形成凭证文档，包括三个部分即需加时间戳的文件摘要；DTS 收到文件日期和时间；DTS 数字签名。

3.1.5 数字凭证

数字凭证称为数字证书，是用电子手段来证实一个用户的身份，对网络资源的访问的权限。在网上电子交易中，如双方出示了各自数字凭证，并用它来进行的交易操作，那么双方都可以不必为对方身份真伪担心。数字凭证有三种类型即个人凭证、企业（服务器）凭证、软件（开发者）凭证。

3.2 身份认证技术

在网络上通过一个具有权威性的和公正性的第三方机构——认证中心，将申请的用户的标识信息（如姓名，身份证号等）与他公钥捆绑在一起，在网络上验证确定其用户身份。前面所提到数字时间戳服务和数字证书发放，也都是由这个认证中心来完成。

3.3 支付网关技术

支付网关，位于公网和传统的银行网络之间（或者终端和收费系统之间），主要功能为：将公网传来数据包解密，并按照银行系统内部通信协议将数据重新就行打包；接收银行系统内部传回的响应消息，数据转换为公网传送的数据格式对其进行加密。支付网关的技术主要完成通信、协议转换和数据加解密的功能，并且可以保护银行内部的网络。此外，支付网关还具有了密码保护和证书管理的其它功能[6]。

3.4 病毒防范技术

电子商务发展，一方面提高了交易的效率，另一方面也为计算机病毒传播创造了条件。计算机的病毒具有不可估量破坏力和威胁性，加强计算机病毒防治工作势在必行。为防范病毒，可以采取以下措施：安装防病毒的软件，加强内部网整体防毒措施；加强数据的备份和恢复措施，做到有备无患；对敏感设备和数据要建立必要物理或逻辑隔离措施等，防患未然。

4 互联网主要的安全协议

4.1 SSL 协议

SSL 协议叫安全套接层协议，面向连接协议，是现在使用的主要协议，当初并非为电子商务而设计。该协议使用了公开密码体制和 X.509 数字证书的技术来保护信息传输机密性和完整性。SSL 协议是在应用层收发数据前，协商加密算法，连接密码而且认证通信双方，为应用层提供了安全传输通道，在该通道上，可透明加载任何高层应用协议以保证了应用层数据传输的安全性。是项基于 TCP/IP 的客户/服务器应用程序，提供了客户端和服务器鉴别、数据完整性及信息机密性的安全措施。协议通过在应用程序，进行数据交换前交换 SSL 初始握手信息，来实现有关安全特性的审查。在 SSL 握手信息中，采用了 DES、MD5 等加密技术，来实现机密性和数据完整性，并采用 X.509 的数字证书来实现鉴别[7]。

4.2 SET 协议

SET 协议叫安全电子交易，对基于信用卡二进行电子化交易的应用，提供了实现安全措施规则，与 SSL 协议比较，做了改进。采用了公钥密码体制和 X.509 数字证书标准，主要应用保障网上购物信息安全性。在商务安全问题中，由于 SET 提供消费者、商家和银行之间的认证，弥补了 SSL 不足，确保了交易数据安全性、完整性、可靠性和交易不可否认性，特别是保证不将消费者银行卡号泄露给商家等优点，它成为目前公认信用卡/借记卡网上交易国际安全标准。除此之外安全超文本传输协议（SHTTP），安全交易技术协议（STT）等等协议为电子商务安全提供了规范。主要是 SET 业务描述、SET 程序员指南和 SET 协议的描述。SET1.0 版已经公布且可应用于任何银行的支付服务。它涵盖了信用卡在电子商务交易中交易协定，信息保密，资料完整及数据认证，数据签名等。

SET 规范明确主要目标是保障付款的安全，确定应用的互通性，使全球市场接受。

4.3 S-HTTP

是对 HTTP 扩充安全特性，增加了报文安全性，是基于 SSL 技术。该协议向 WWW 应用提供完整性，鉴别，不可抵赖性及机密性等安全措施[8]。

5 电子商务安全管理对策

电子商务安全管理，不应只是从单纯技术的角度考虑如何解决问题，而应该从综合安全管理思路来考虑，因从电子商务运行环境来看，技术环境只是一个重要方面。

5.1 加强技术保证，确保电子商务的安全

电子商务运作涉及资金安全，货物安全，信息安全，商业秘密等多方面安全问题，任何一点漏洞可能导致大量的资金流失，这些安全首先对信息技术的依赖。对如何保障企业信息数据和重大商业机密，也是确保开展电子商务的企业重要技术保障和前提，只有高度重视电子商务信息安全，才能确保其运行安全，这需要有强大技术安全保障措施，不仅要制定完善技术保障措施，更要严格的执行制度，才能确保电子商务信息安全[9]。

5.2 健全内部控制制度

实行电子商务商户，在内部管理上应健全相应规章制度，通过制定制度来规范和约束员工行为，根据其工作重要程度，确定该系统安全等级。制订机房出入管理制度相对于安全等级要求较高的系统，实行分区控制，限制工作人员出入无关的区域。对操作规程也要根据职责分离和多人负责原则，各负其责，不能超越自己管辖范围；制订完备系统维护制度，对系统进行维护，要采取数据保护措施。

5.3 加强电子商务安全的管理措施

5.3.1 提高网络安全防范意识

虽然许多企业建立了技术防范机制，运用先进适用的信息安全技术，建造起一道道屏障，阻隔了罪犯或竞争对手的入侵，防范和化解了风险，保证了电子商务的顺利进行。但没有意识到互联网易受攻击性，目前国内网站存在安全问题，其主要原因是企业管理者缺少安全意识。

5.3.2 建立电子商务安全管理组织体系

完善组织体系应根据企业目标和安全方针，建立信息安全指导委员会。委员会由企业高层领导挂帅，各职能部分负责人参加，要定期召开会议，对组织内的信息安全问题，进行讨论并作为决策，为组织信息安全提供支持，主要职能有是审批信息安全方针，政策，分配安全管理职责，确认风险评估，审批安全预算计划及设施的购置，评审与监测信息措施的实施及安全事故处理对与信息安全管理的重大更改事项进行决策，协调与各部门之间的关系。

5.3.3 加强电子商务法律体系的建设

电子商务在交易过程中存在法律风险，电子商务是在网络进行的，电子商务交易是无纸贸易，是一个虚拟环境交易，对这些虚拟交易的法律监管并不完善，这些问题使电子商务认证、交易有不受法律保护的风险。另外，电子商务还存在知识产权风险。网络是个开放平台，资源在网络中传播是畅通的。在网络中资源共享性使得知识产权的资源受保护力度被降低，可能带来电子商务交易知识产权纠纷等法律风险问题。我国立法部门要立足国情，吸取和借鉴外国立法先进经验，加快我国立法进程，早日使我国电子商务安全走上法制化轨道。电子商务法律建设也是一项非常复杂系统工程，它包括了立法、司法和行政诸多方面，涵盖了行业市场准入、信息安全认证、知识产权的保护、电子支付、数字签名、互联网内容的管理及赔偿责任诸多法律问题[10]。

6 结语

安全是电子商务的核心，电子商务对网络安全与商务安全双重要求，使网络安全与商务安全是密不可分。没有计算机网络的安全作为基础，商务交易安全就是空中楼阁，无从谈起；没有商务安全保障，计算机网络本身再安全，也无法达到电子商务所特有的安全的要求，电子商务相应实现技术和各种协议，正是安全得以实现的保证。

快捷的电子商务，在给企业带来了发展机遇的同时，也使企业面临各种安全风险。由于缺乏电子商务信息安全管理的系统认识，很多企业把其电子商务信息安全，作为一项技术工程来实施，忽略了交易过程中的各种参与人员对安全的影响。分析企业在电子商务安全的管理体制方面存在不足和原因，从安全防范的意识、管理组织体系、信息安全的技术策略、人员的管理与培训、电子商务的立法等方面提出了一些加强人员的安全管理建议。现代企业走向电子商务的时代，只有管理与技术的并重，才能确保企业在电子商务交易过程中的信息安全。

参考文献：

[1]黄京华电子商务教程[N].北京：清华大学出版社，2003.

[2]王健电子商务[N].上海：海天出版，2003.

[3]姚国章.中国企业电子商务发展战略[N].北京大学出版社，2011.

[4]高延鹏，刘林林.中小企业电子商务发展问题与对策研究[J]潍坊学院学报，2008（03）.

[5]李钢《我国中小企业实施电子商务发展问题与对策》[J]中小企业管理与科技，2007（01）.

[6]陈爱国《中小企业电子商务发展现状与对策研究》[J]河南商业高等专科学校学报，2007（01）.

[7]朱保平我国中小企业发展电子商务的现状及对策研究[J]新西部（下半月），2007（08）.

[8]赵春雨中小企业开展电子商务的现状与发展[J]市场周刊（理论研究），2007（06）.

[9]方美琪.电子商务概论[N].北京：清华大学出版社，2009 年.

[10]刘光明.中外企业文化案例[N].北京：经济管理出版社，2010.7.

作者简介：王彬（1983.2-），男，上海人，人社部高级考评员，FIPA 澳大利亚注册资深公共会计师，FFA 英国注册资深财务会计师，CISA 国际注册信息系统审计师，PMP 美国注册项目管理专业人士资格认证，建筑防护设计高级工程师，中式烹调师一级，ChFP 高级理财规划师一级，高级人力资源管理师，CIWM 国际财富管理师，CICFP 注册理财规划师，中级给排水工程师，心理咨询师二级，国家二级教师，助理药师，计算机维修工三级，计算机操作员三级，电子商务师三级，二手车评估师三级，助理 IFM，毕业于华东师范大学电子商务本科、北京大学医学院药学本科、西南财经大学会计学本科，中国地质大学艺术设计本科、海口经济学院财务管理本科，NYIT（美国纽约理工学院）MBA，国家机关事务局与清华大学联合举办的全国公共机构节能管理项目结业。中国科学技术协会中国未来研究会理事会理事。中国建筑业协会会员。中国建筑学会会员。上海市建筑学会生态建设专业委员会会员。四川城乡人才服务中心会员。中博联智库特聘专家。上海任蕴教育科技有限公司、启恋建筑设计事务所（上海）有限公司、任防建筑设计事务所（上海）有限公司人防防护工程研究员。海南科技职业大学教授。主要研究方向为人防工程。