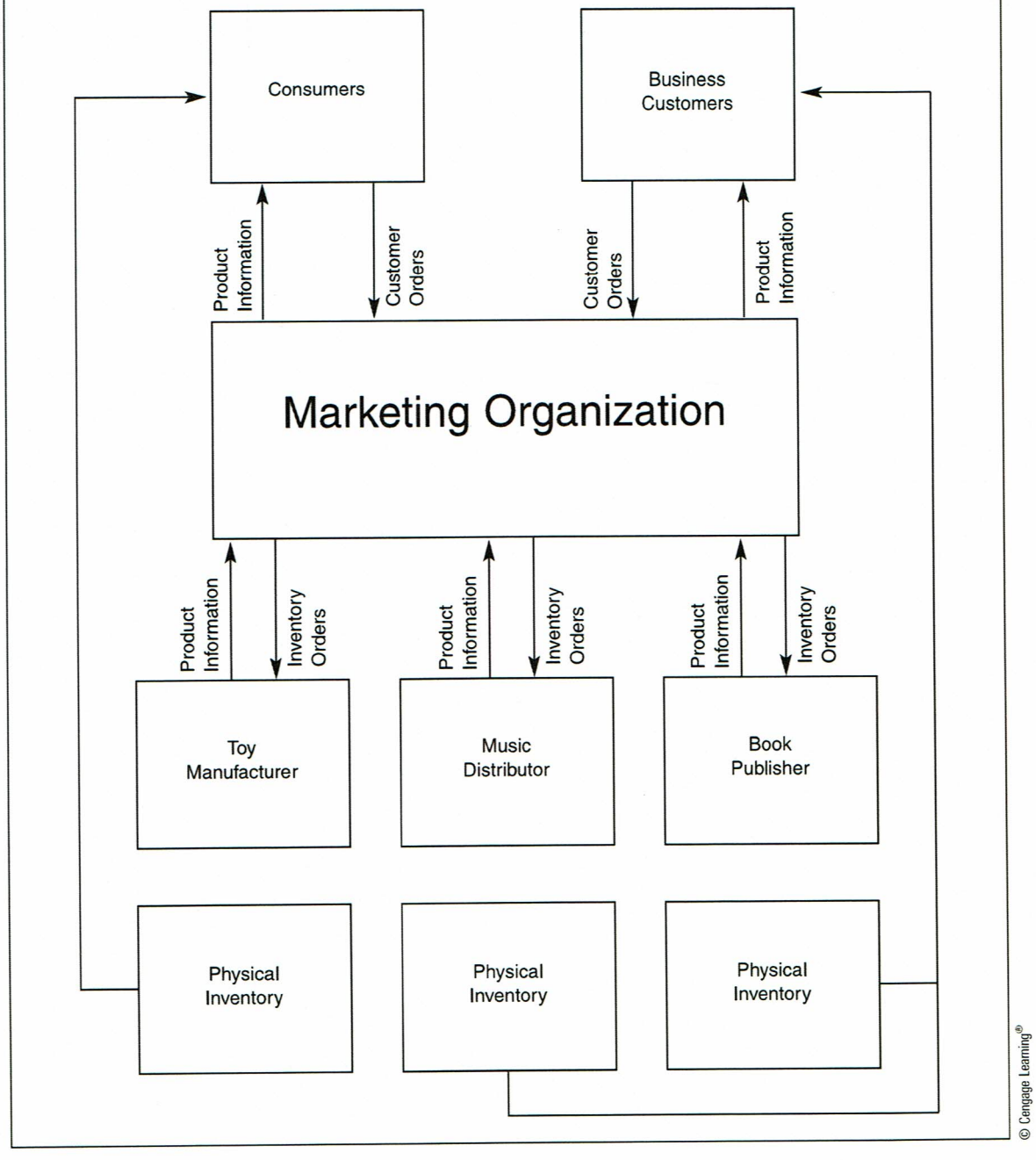
FIGURE 12-2 DYNAMIC VIRTUAL ORGANIZATION



The selling organization maintains a website for advertising product offerings. The products themselves are not physically in the custody of the seller but are stored at the facilities of the trading partner (e.g., manufacturer, publisher, or distributor). The seller provides customers with product descriptions, consumer reports, prices, availability, and expected delivery times. This information comes from trading partners through an Internet connection. The seller validates customer orders placed through the website and automatically dispatches these to the trading partner firm, which actually ships the product.

The virtual organization can expand, contract, or shift its product line and services by simply adding or eliminating trading partners. To fully exploit this flexibility, organizations often forge relationships with total strangers. Managers in both firms need to make quick determinations as to the competence, compatibility, and capacity of potential partners to discharge their responsibilities. These and other security-related risks are potential impediments to electronic commerce.

Risks Associated with Electronic Commerce

Reliance on electronic commerce poses concern about unauthorized access to confidential information. As LANs become the platform for mission-critical applications and data, proprietary information, customer data, and financial records are at risk. Organizations connected to their customers and business partners via the Internet are particularly exposed. Without adequate protection, firms open their doors to computer hackers, vandals, thieves, and industrial spies, both internally and from around the world.

The paradox of networking is that networks exist to provide user access to shared resources, yet the most important objective of any network is to control such access. Hence, for every productivity argument in favor of remote access, there is a security argument against it. Organization management constantly seeks balance between increased access and the associated business risks.

In general, business **risk** is the possibility of loss or injury that can reduce or eliminate an organization's ability to achieve its objectives. In terms of electronic commerce, risk relates to the loss, theft, or destruction of data as well as the use of computer programs that financially or physically harm an organization. The following sections deal with various forms of risk. This includes intranet risks posed by dishonest employees who have the technical knowledge and the position to perpetrate frauds, and Internet risks that threaten both consumers and business entities.

INTRANET RISKS

Intranets consist of small LANs and large WANs that may contain thousands of individual nodes.[3] Intranets are used to connect employees within a single building, between buildings on the same physical campus, and between geographically dispersed locations. Typical intranet activities include e-mail routing, transaction processing between business units, and linking to the outside Internet.

Unauthorized and illegal employee activities internally spawn intranet threats. Their motives for doing harm may be vengeance against the company, the challenge of breaking into unauthorized files, or to profit from selling trade secrets or embezzling assets. The threat from employees (both current and former) is significant because of their intimate knowledge of system controls and/or the lack of controls. Discharged employees, or those who leave under contentious circumstances, raise particular concerns. Trade secrets, operations data, accounting data, and confidential information to which the employee has access are at greatest risk.

Interception of Network Messages

The individual nodes on most intranets are connected to a shared channel across which travel user IDs, passwords, confidential e-mails, and financial data files. The unauthorized interception of this information by a node on the network is called sniffing. The exposure is even greater when the intranet is connected to the Internet. Network administrators routinely use commercially available sniffer software to analyze network traffic and to detect bottlenecks. Sniffer software, however, can also be downloaded from the Internet. In the hands of a computer criminal, sniffer software can be used to intercept and view data sent across a shared intranet channel.

Privileged Employees with Access to Corporate Databases

Intranets connected to central corporate databases increase the risk that an employee will view, corrupt, change, or copy data. Outsiders may bribe employees who have access privileges to digital financial accounts to write-off an account receivable or sell sensitive information such as social security

3 See the chapter appendix for a complete discussion of LANs and WANs.

numbers, customer listings, credit card information, recipes, formulas, and design specifications. In 2010 the FBI charged two GM employees with downloading and stealing thousands of GM documents regarding the company's hybrid technology worth an estimated 40 million dollars. The employees offered this information to an automotive manufacturer based in China and a competitor of GM.

Reluctance to Prosecute

A factor that contributes to computer crime is the reluctance on the part of many victim organizations to prosecute the criminals because of fear of negative publicity. By pursuing prosecution in public court, a victim organization will necessarily expose its weaknesses in policy, procedures, and internal control to its customers, suppliers, and other business partners. Apart from the public criticism that such disclosures will likely provoke, customers may abandon the firm, and trading partners may impose greatly restrictive business practices on it.

Many computer criminals are repeat offenders, and performing background checks on prospective employees can significantly reduce an organization's hiring risk and avoid criminal acts. In the past, employee background checking was difficult to achieve because former employers, fearing legal action, were reluctant to disclose negative information to prospective employers. A "no comment" policy prevailed.

The legal doctrine of negligent hiring liability is changing this. This doctrine effectively requires employers to check into an employee's background. Increasingly, courts are holding employers responsible for criminal acts that employees, both on and off the job, perpetrated if a background check could have prevented crimes. Many states have passed laws that protect a former employer from legal action when providing work-related performance information about a former employee when (1) the inquiry comes from a prospective employer, (2) the information is based on credible facts, and (3) the information is given without malice.

INTERNET RISKS

This section looks at some of the more significant risks associated with Internet commerce. First, the risks related to consumer privacy and transaction security are examined. The risks to business entities from fraud and malicious acts are then reviewed.

RISKS TO CONSUMERS

As more and more people connect to the web, Internet fraud increases. Because of this, many consumers view the Internet as an unsafe place to do business. In particular, they worry about the security of credit card information left on websites and the confidentiality of their transactions. Some of the more common threats to consumers from cyber criminals are discussed here.

THEFT OF CREDIT CARD NUMBERS. The perception that the Internet is not secure for credit card purchases is considered to be the biggest barrier to electronic commerce. Some Internet companies are negligent or even fraudulent in the way they collect, use, and store credit card information. One hacker successfully stole 100,000 credit card numbers with a combined credit limit of $1 billion from an Internet service provider's customer files. He was arrested when he tried to sell the information to an undercover FBI agent.

Another fraud scheme involves establishing a fraudulent business operation that captures credit card information. For example, the company may take orders to deliver flowers on Mother's Day. When the day arrives, the company goes out of business and disappears from the web. Of course, the flowers are never delivered, and the perpetrator either sells or uses the credit card information.

THEFT OF PASSWORDS. One form of Internet fraud involves establishing a website to steal a visitor's password. To access the web page, the visitor is asked to register and provide an e-mail address and password. Many people use the same password for different applications such as ATM services, e-mail, and employer-network access. In the hopes that the website visitor falls into this pattern of behavior, the cyber criminal uses the captured password to break into the victim's accounts.

CONSUMER PRIVACY. Concerns about the lack of privacy discourage many consumers from engaging in Internet commerce. One aspect of privacy involves the way in which websites capture and use cookies.

Cookies are files containing user information that are created by the web server of the site being visited. The cookies are then stored on the visitor's computer hard drive. They contain the URLs of visited sites. When the site is revisited, the user's browser sends the specific cookies to the web server. The original intent behind the cookie was to improve efficiency in processing return visits to sites where users are required to register for services. For example, on the user's first visit to a particular website, the URL and user ID may be stored as a cookie. On subsequent visits, the website retrieves the user ID, thus saving the visitor from rekeying the information.

Cookies allow websites to off-load the storage of routine information about vast numbers of visitors. It is far more efficient for a web server to retrieve this information from a cookie file stored on the user's computer than to search through millions of such records stored at the website. Most browsers have preference options to disable cookies or to warn the user before accepting one.

The privacy controversy over cookies relates to what information is captured and how it is used. For example, the cookie may be used to create a profile of user preferences for marketing purposes. The profile could be based on the pages accessed or the options selected during the site visit, the time of day or night of the visit, and the length of time spent at the site. The profile could also include the user's e-mail address, zip code, home phone number, and any other information the user is willing to provide to the website.

This type of information is useful to online marketing firms that sell advertising for thousands of Internet firms. The user profile enables the marketing firm to customize ads and to target them to Internet consumers. To illustrate, let's assume a user visiting an online bookstore browses sports car and automobile racing listings. This information is stored in a cookie and transmitted to the online marketing firm, which then sends JavaScript ads for general automotive products to the bookstore's web page to entice the visitor to click on the ads. Each time the consumer visits the site, the contents of the cookie will be used to trigger the appropriate ads. User profile information can also be compiled into a mailing list, which is sold and used in the traditional way for solicitation.

Risks to Businesses

Business entities are also at risk from Internet commerce. IP spoofing, denial of service attacks, and malicious programs are three significant concerns.

IP SPOOFING. IP spoofing is a form of masquerading to gain unauthorized access to a web server and/or to perpetrate an unlawful act without revealing one's identity. To accomplish this, a perpetrator modifies the IP address of the originating computer to disguise his or her identity. A criminal may use IP spoofing to make a message appear to be coming from a trusted or authorized source and thus slip through control systems designed to accept transmissions from certain (trusted) host computers and block out others. This technique could be used to crack into corporate networks to perpetrate frauds, conduct acts of espionage, or destroy data. For example, a hacker may spoof a manufacturing firm with a false sales order that appears to come from a legitimate customer. If the spoof goes undetected, the manufacturer will incur the costs of producing and delivering a product that was never ordered.

DENIAL OF SERVICE ATTACK. A **denial of service attack (DoS)** is an assault on a web server to prevent it from servicing its legitimate users. Although such attacks can be aimed at any type of website, they are particularly devastating to business entities that are prevented from receiving and processing business transactions from their customers. Three common types of DoS attacks are: SYN flood, smurf, and distributed denial of service (DDoS).

SYN FLOOD ATTACK. When a user establishes a connection on the Internet through TCP/IP, a three-way handshake takes place. The connecting server sends an initiation code called a SYN (SYNchronize) packet to the receiving server. The receiving server then acknowledges the request by returning a **SYNchronize-ACKnowledge (SYN-ACK)** packet. Finally, the initiating host

machine responds with an ACK packet code. The **SYN flood attack** is accomplished by not sending the final acknowledgment to the server's SYN-ACK response, which causes the server to keep signaling for acknowledgement until the server times out.

The individual or organization perpetrating the SYN flood attack transmits hundreds of SYN packets to the targeted receiver, but never responds with an ACK to complete the connection. As a result, the ports of the receiver's server are clogged with incomplete communication requests that prevent legitimate transactions from being received and processed. Organizations under attack thus may be prevented from receiving Internet messages for days at a time.

If the target organization could identify the server that is launching the attack, a firewall (discussed later) could be programmed to ignore all communication from that site. Such attacks, however, are difficult to prevent because they use IP spoofing to disguise the source of the messages. IP spoofing programs that randomize the source address of the attacker have been written and publicly distributed over the Internet. Therefore, to the receiving site, it appears that the transmissions are coming from all over the Internet.

SMURF ATTACK. A **smurf attack** involves three parties: the perpetrator, the intermediary, and the victim. It is accomplished by exploiting an Internet maintenance tool called a **ping**, which is used to test the state of network congestion and determine whether a particular host computer is connected and available on the network. The ping works by sending an echo request message (like a sonar ping) to the host computer and listening for a response message (echo reply). The ping signal is encapsulated in a message packet that also contains the return IP address of the sender. A functioning and available host must return an echo reply message that contains the exact data received in the echo request message packet.

The perpetrator of a smurf attack uses a program to create a ping message packet that contains the forged IP address of the victim's computer (IP spoofing) rather than that of the actual source computer. The ping message is then sent to the intermediary, which is actually an entire subnetwork of computers. By sending the ping to the network's **IP broadcast address**, the perpetrator ensures that each node on the intermediary network receives the echo request automatically. Consequently, each intermediary node sends echo responses to the ping message, which are returned to the victim's IP address, not that of the source computer. The resulting flood echoes can overwhelm the victim's computer and cause network congestion that makes it unusable for legitimate traffic. Figure 12-3 illustrates a smurf attack.

The intermediary in a smurf attack is an unwilling and unaware party. Indeed, the intermediary is also a victim and to some extent suffers the same type of network congestion problems the target victim suffers. One method of defeating smurf attacks is to disable the IP broadcast addressing option at each network firewall and thus eliminate the intermediary's role. In response to this move, however, attackers have developed tools to search for networks that do not disable broadcast addressing. These networks may subsequently be used as intermediaries in smurf attacks. Also, perpetrators have developed tools that enable them to launch smurf attacks simultaneously from multiple intermediary networks for maximum effect on the victim.

DISTRIBUTED DENIAL OF SERVICE. A **distributed denial of service (DDoS)** attack may take the form of a SYN flood or smurf attack. The distinguishing feature of the DDoS is the sheer scope of the event. The perpetrator of a DDoS attack may employ a virtual army of so-called **zombie** or bot (robot) computers to launch the attack. Because vast numbers of unsuspecting intermediaries are needed, the attack often involves one or more **Internet Relay Chat (IRC)** networks as a source of zombies. IRC is a popular interactive service on the Internet that lets thousands of people from around the world engage in real-time communications via their computers.

The problem with IRC networks is that they tend to have poor security. The perpetrator can thus easily access the IRC and upload a malicious program, such as a Trojan horse (see the appendix in Chapter 16 for a definition), which contains DDoS attack script. This program is subsequently downloaded to the PCs of the many thousands of people who visit the IRC site. The attack program runs in the background on the new zombie computers, which are now under the control of the perpetrator. These collections of compromised computers are known as **botnets.** Figure 12-4 illustrates this technique.

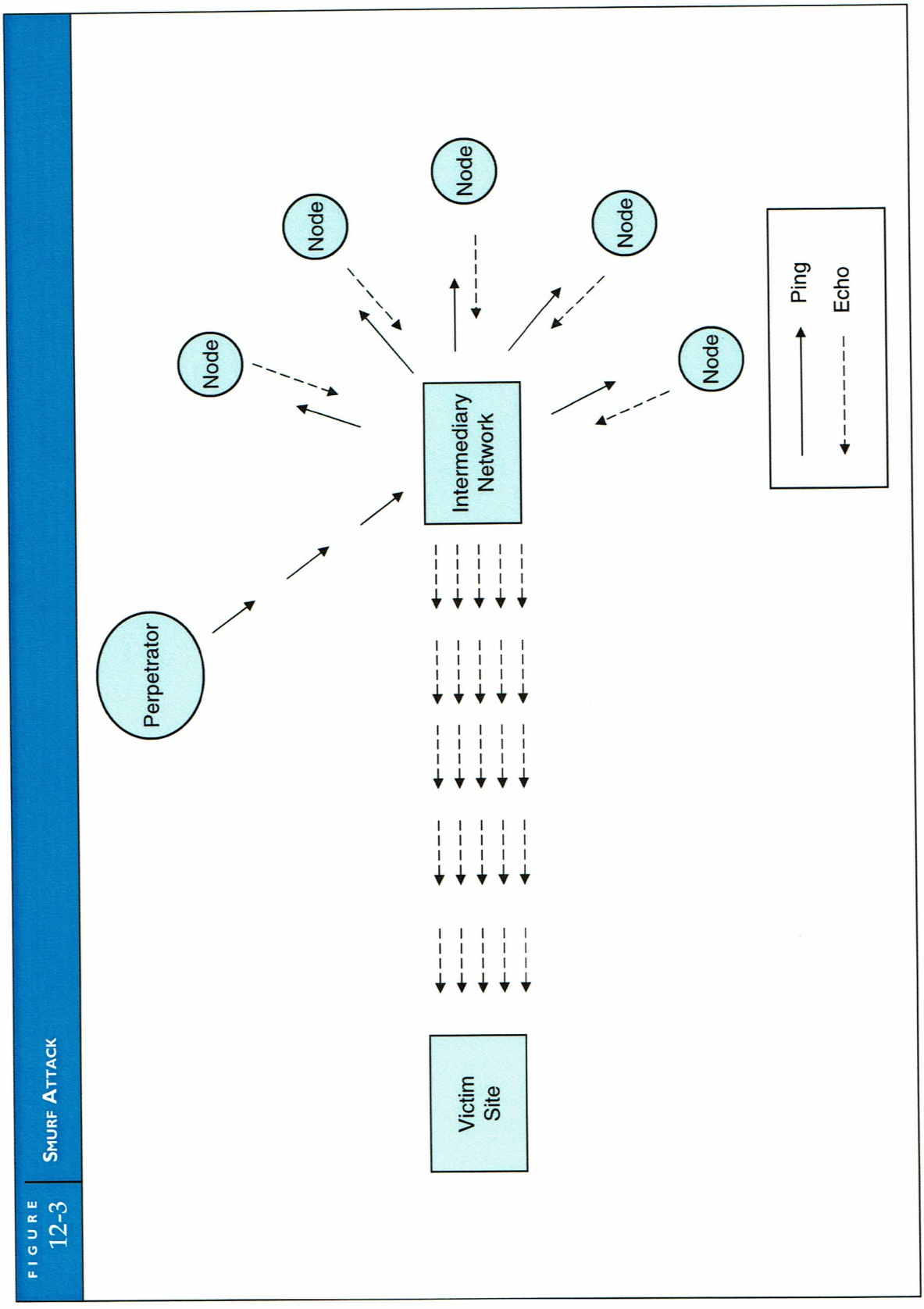
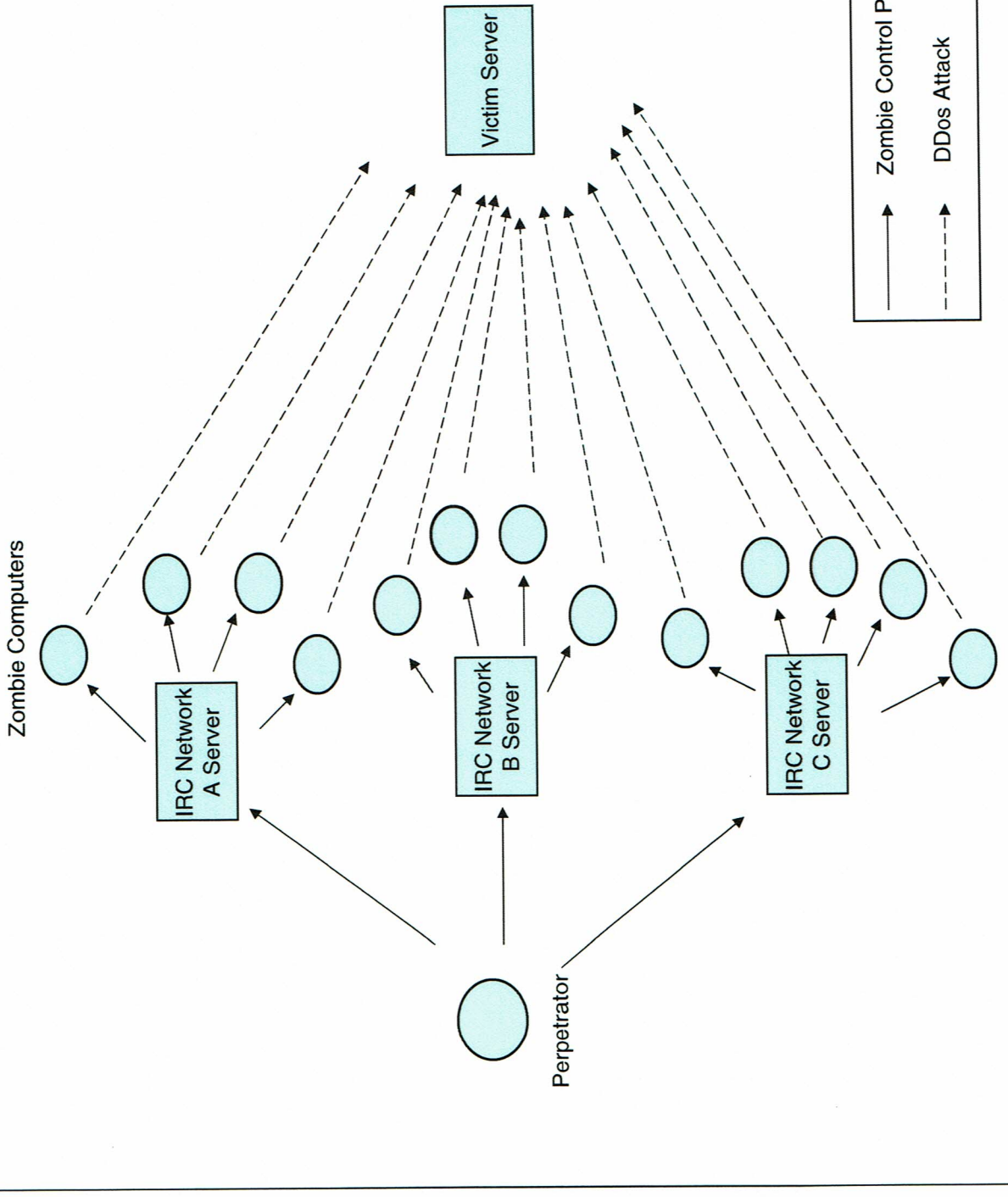


FIGURE 12-3 SMURF ATTACK

FIGURE 12-4 DISTRIBUTED DENIAL OF SERVICE ATTACK



Via the zombie control program, the perpetrator has the power to direct the DDoS to specific victims and turn on or off the attack at will. The DDoS attack poses a far greater threat to the victim than a traditional SYN flood or smurf attack. For instance, a SYN flood coming from thousands of distributed computers can do far more damage than one from a single computer. Also, a smurf attack coming from a subnetwork of intermediary computers all emanate from the same server. In time, the server can be located and isolated by programming the victim's firewall to ignore transmissions from the attacking site. The DDoS attack, on the other hand, literally comes from sites all across the Internet. Thousands of individual attack-computers are harder to track down and turn off.

MOTIVATION BEHIND DOS ATTACKS. The motivation behind DoS attacks may originally have been to punish an organization with which the perpetrator had a grievance or simply to gain bragging rights for being able to do it. Today, DoS attacks are also perpetrated for financial gain. Financial institutions, which are particularly dependent on Internet access, have been prime targets. Organized criminals threatening a devastating attack have extorted several institutions, including the Royal Bank of Scotland. The typical scenario is for the perpetrator to launch a short DDoS attack (a day or so) to demonstrate what life would be like if the organization were isolated from the Internet. During this time, legitimate customers are unable to access their online accounts and the institution is unable to process many financial transactions. After the attack, the CEO of the organization receives a phone call demanding that a sum of money be deposited in an offshore account, or the attack will resume. Compared to the potential loss in customer confidence, damaged reputation, and lost revenues, the ransom may appear to be a small price to pay. DDoS attacks are relatively easy to execute and can have a devastating effect on the victim. Many experts believe that the best defense against DDoS attacks is to implement a layered security program with multiple detection point capability. We revisit this issue in Chapter 16 to examine methods for dealing with DDoS attacks.

OTHER MALICIOUS PROGRAMS. Viruses and other forms of malicious programs, such as worms, logic bombs, and Trojan horses, pose a threat to both Internet and intranet users. These may be used to bring down a computer network by corrupting its operating systems, destroying or corrupting corporate databases, or capturing passwords that enable hackers to break in to the system. Malicious programs, however, are not exclusively an electronic commerce issue; database management, operating systems security, and application integrity are also threatened. Because of the broad-based implications, this class of risk is examined at length in Chapter 16.

Security, Assurance, and Trust

Trust is the catalyst for sustaining electronic commerce. Both consumers and businesses are drawn to organizations that are perceived to have integrity. Organizations must convey a sense that they are competent and conduct business fairly with their customers, trading partners, and employees. This is a two-pronged problem. First, the company must implement the technological infrastructure and controls needed to provide for adequate security. Second, the company must assure potential customers and trading partners that adequate safeguards are in place and working. A large part of data security involves data encryption, digital authentication, and firewalls. These security techniques are outlined in the following section but are presented in more detail in Chapter 16. This section concludes with a review of seals of assurance techniques that promote trust in electronic commerce.

ENCRYPTION

Encryption is the conversion of data into a secret code for storage in databases and transmission over networks. The sender uses an encryption algorithm to convert the original message (called cleartext) into a coded equivalent (called ciphertext). At the receiving end, the ciphertext is decoded (decrypted) back into cleartext.

The earliest encryption method is called the **Caesar cipher**, which Julius Caesar is said to have used to send coded messages to his generals in the field. Like modern-day encryption, the Caesar cipher has two fundamental components: a key and an algorithm.

The **key** is a mathematical value that the sender selects. The **algorithm** is the procedure of shifting each letter in the cleartext message the number of positions that the key value indicates. Thus, a key value of +3 would shift each letter three places to the right. For example, the letter A in cleartext would be represented as the letter D in the ciphertext message. The receiver of the ciphertext message reverses the process to decode it and recreates the cleartext, in this case shifting each ciphertext letter three places to the left. Obviously, both the sender and receiver of the message must know the key.

Modern-day encryption algorithms, however, are far more complex, and encryption keys may be up to 128 bits in length. The more bits in the key, the stronger the encryption method. Today, nothing less than 128-bit algorithms are considered truly secure. Two commonly used methods of encryption are private key and public key encryption.

Advanced encryption standard (AES), also known as Rijndael, is a **private key** (or **symmetric key**) encryption technique. The U.S. government has adopted it as an encryption standard. To encode a message, the sender provides the encryption algorithm with the key, which produces the ciphertext message. This is transmitted to the receiver's location, where it is decoded using the same key to produce a cleartext message. Because the same key is used for coding and decoding, control over the key becomes an important security issue. The more individuals that need to exchange encrypted data, the greater the chance that the key will become known to an intruder who could intercept a message and read it, change it, delay it, or destroy it.

To overcome this problem, **public key encryption** was devised. This approach uses two different keys: one for encoding messages and the other for decoding them. The recipient has a private key used for decoding, which is kept secret. The encoding key is public and published for everyone to use. This approach is illustrated in Figure 12-5.

Receivers never need to share private keys with senders, which reduces the likelihood that they fall into the hands of an intruder. One of the most trusted public key encryption methods is **Rivest-Shamir-Adleman (RSA).** This method is, however, computationally intensive and much slower than private key encryption. Sometimes, both private key and public key encryption are used together in what is called a **digital envelope.**

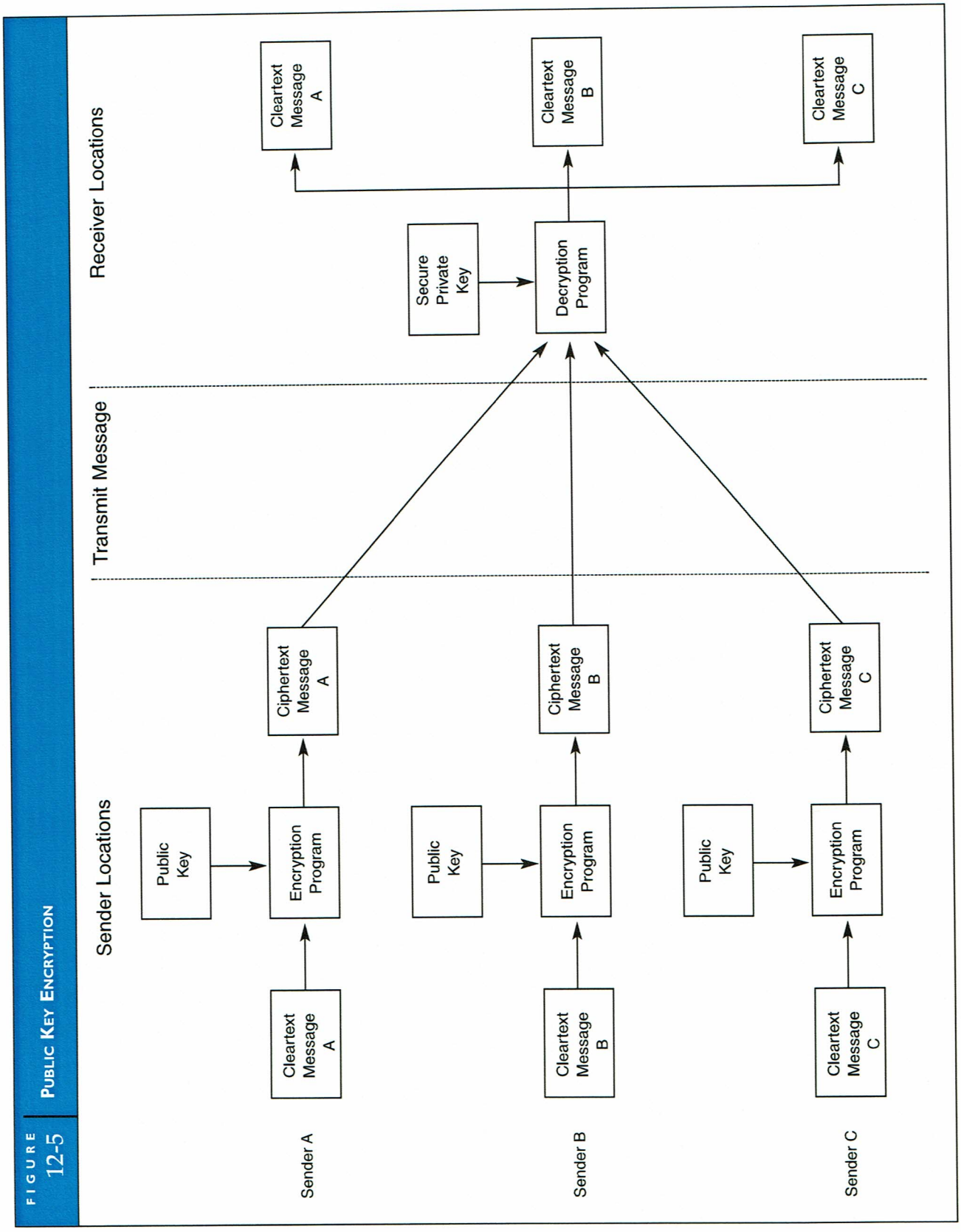
DIGITAL AUTHENTICATION

Encryption alone cannot resolve all security concerns. For example, how does the supplier (receiver) know for sure that a hacker did not intercept and alter a customer's (sender) purchase order (message) for 1,000 units of product to read 100,000? If such an alteration went undetected, the supplier would incur the labor, material, manufacturing, and distribution costs for the order. Litigation between the innocent parties may ensue.

A **digital signature** is an electronic authentication technique that ensures the transmitted message originated with the authorized sender and that it was not tampered with after the signature was applied. The digital signature is derived from a mathematically computed digest of the document that has been encrypted with the sender's private key. Both the digital signature and the text message are encrypted using the receiver's public key and transmitted to the receiver. At the receiving end, the message is decrypted using the receiver's private key to produce the digital signature (encrypted digest) and the cleartext version of the message. Finally, the receiver uses the sender's public key to decrypt the digital signal to produce the digest. The receiver recalculates the digest from the cleartext using the original hashing algorithm and compares this to the transmitted digest. If the message is authentic, the two digest values will match. If even a single character of the message was changed in transmission, the digest figures will not be equal.

Another concern facing the receiver is determining if the expected sender actually initiated a message. For example, suppose that the supplier receives a purchase order addressed from Customer A for 100,000 units of product, which was actually sent from an unknown computer criminal. Once again, significant costs would accrue to the supplier if it acts on this fraudulent order.

FIGURE 12-5 PUBLIC KEY ENCRYPTION



A **digital certificate** is like an electronic identification card that is used in conjunction with a public key encryption system to verify the authenticity of the message sender. Trusted third parties known as **certification authorities** (CAs) (e.g., Veri-Sign, Inc.) issue digital certificates, also called digital IDs. The digital certificate is actually the sender's public key that the CA has digitally signed. The digital certificate is transmitted with the encrypted message to authenticate the sender. The receiver uses the CA's public key to decrypt the sender's public key, which is attached to the message, and then uses the sender's public key to decrypt the actual message.

Because public key encryption is central to digital authentication, public key management becomes an important internal control issue. **Public key infrastructure (PKI)** constitutes the policies and procedures for administering this activity. A PKI system consists of:

1. A certification authority that issues and revokes digital certificates.
2. A registration authority that verifies the identity of certificate applicants. The process varies depending on the level of certification desired. It involves establishing one's identity with formal documents, such as a driver's license, notarization, fingerprints, and proving one's ownership of the public key.
3. A certification repository, which is a publicly accessible database that contains current information about current certificates and a certification revocation list of certificates that have been revoked and the reasons for revocation.

FIREWALLS

A **firewall** is a system used to insulate an organization's intranet from the Internet. It can be used to authenticate an outside user of the network, verify his or her level of access authority, and then direct the user to the program, data, or service requested. In addition to insulating the organization's network from external networks, firewalls can also be used to protect LANs from unauthorized internal access.

A common configuration employs two firewalls: a network-level firewall and an application-level firewall. The **network-level firewall** provides basic screening of low-security messages (for example, e-mail) and routes them to their destinations based on the source and destination addresses attached. The **application-level firewall** provides high-level network security. These firewalls are configured to run security applications called proxies that perform sophisticated functions, such as verifying user authentication.

SEALS OF ASSURANCE

In response to consumer demand for evidence that a web-based business is trustworthy, a number of trusted third-party organizations are offering seals of assurance that businesses can display on their website home pages. To legitimately bear the seal, the company must show that it complies with certain business practices, capabilities, and controls. This section reviews six seal-granting organizations: Better Business Bureau (BBB), TRUSTe, Veri-Sign, Inc., International Computer Security Association (ICSA), AICPA/CICA WebTrust, and AICPA/CICA SysTrust.

Better Business Bureau

The BBB is a nonprofit organization that has been promoting ethical business practices through self-regulation since 1912. The BBB has extended its mission to the Internet through a wholly owned subsidiary called BBBOnline, Inc. To qualify for the BBBOnline seal, an organization must:

- Become a member of the BBB.
- Provide information about the company's ownership, management, address, and phone number. This is verified by a physical visit to the company's premises.
- Be in business for at least one year.
- Promptly respond to customer complaints.
- Agree to binding arbitration for unresolved disputes with customers.

The assurance BBBOnline provides relates primarily to concern about business policies, ethical advertising, and consumer privacy. BBBOnline does not verify controls over transaction processing integrity and data security issues.

TRUSTe

Founded in 1996, TRUSTe is a nonprofit organization dedicated to improving consumer privacy practices among Internet businesses and websites. To qualify for the TRUSTe seal, the organization must:

- Agree to follow TRUSTe privacy policies and disclosure standards.
- Post a privacy statement on the website disclosing the type of information being collected, the purpose for collecting information, and with whom it is shared.
- Promptly respond to customer complaints.
- Agree to site compliance reviews by TRUSTe or an independent third party.

TRUSTe addresses consumer privacy concerns exclusively and provides a mechanism for posting consumer complaints against its members. If a member organization is found to be out of compliance with TRUSTe standards, its right to display the trust seal may be revoked.

Veri-Sign, Inc.

Veri-Sign, Inc., was established as a for-profit organization in 1995. It provides assurance regarding the security of transmitted data. The organization does not verify security of stored data or address concerns related to business policies, business processes, or privacy. Its mission is to provide digital certificate solutions that enable trusted commerce and communications. Their products allow customers to transmit encrypted data and verify the source and destination of transmissions. Veri-Sign, Inc., issues three classes of certificates to individuals, businesses, and organizations. To qualify for class three certification, the individual, business, or organization must provide a third-party confirmation of name, address, telephone number, and website domain name.

International Computer Security Association

The ICSA established its web certification program in 1996. ICSA certification addresses data security and privacy concerns. It does not deal with concerns about business policy and business processes. Organizations that qualify to display the ICSA seal have undergone an extensive review of firewall security from outside hackers. Organizations must be recertified annually and undergo at least two surprise checks each year.

AICPA/CICA WebTrust

The AICPA and CICA established the WebTrust program in 1997. To display the AICPA/CICA Web-Trust seal, the organization undergoes an examination according to the AICPA's Standards for Attestation Engagements, No. 1, by a specially web-certified CPA or CA. The examination focuses on the areas of business practices (policies), transaction integrity (business process), and information protection (data security). The seal must be renewed every 90 days.

AICPA/CICA SysTrust

In July 1999, the AICPA/CICA introduced an exposure draft describing a new assurance service called SysTrust. It is designed to increase management, customer, and trading partner confidence in systems that support entire businesses or specific processes. The assurance service involves the public accountant evaluating the system's reliability against four essential criteria: availability, security, integrity, and maintainability.

The potential users of SysTrust are trading partners, creditors, shareholders, and others who rely on the integrity and capability of the system. For example, Virtual Company is considering outsourcing some of its vital functions to third-party organizations. Virtual needs assurance that the third-party systems are reliable and adequate to provide the contracted services. As part of

the outsourcing contract, Virtual requires the servicing organizations to produce a clean SysTrust report every three months.

In theory, the SysTrust service will enable organizations to differentiate themselves from their competitors. Those organizations that undergo a SysTrust engagement will be perceived as competent service providers and trustworthy. They will be more attuned to the risks in their environment and equipped with the necessary controls to deal with the risks.[4]

Implications for the Accounting Profession

The issues discussed in this chapter carry many implications for auditors and the public accounting profession. As mission-critical functions, such as inventory procurement, sales processing, shipping notification, and cash disbursements, are performed automatically, digitally, and in real time, auditors are faced with the challenge of developing new techniques for assessing control adequacy and verifying the occurrence and accuracy of economic events. The following describes issues of increasing importance to auditors in the electronic commerce age.

PRIVACY VIOLATION

Privacy pertains to the level of confidentiality that an organization employs in managing customer and trading partner data. Privacy applies also to data that web sites collect from visitors who are not customers. Specific concerns include:

- Does the organization have a stated privacy policy?
- What mechanisms are in place to ensure the consistent application of stated privacy policies?
- What information on customers, trading partners, and visitors does the company capture?
- Does the organization share or sell its customer, trading partner, or visitor information?
- Can individuals and business entities verify and update the information captured about them?

The **Safe Harbor Agreement** implemented in 1995 addresses the importance of privacy. The two-way agreement between the United States and the European Union establishes standards for information transmittal. Approved by the European Commission in July 2000, the Safe Harbor principles essentially enable U.S. companies to do business in the European Union by establishing what is deemed to be an adequate level of privacy protection. Although the document is still evolving, it establishes that companies need to enter the Safe Harbor Agreement or provide evidence that they are abiding by the privacy regulations set forth in it. Noncompliant organizations may be effectively banned from doing business in the European Union. Compliance with the Safe Harbor Agreement requires that a company meet six conditions that are described next.[5]

NOTICE. Organizations must provide individuals with clear notice of "the purposes for which it collects and uses information about them, the types of third parties to which it discloses the information, and how to contact the company with inquiries or complaints."

CHOICE. Before any data are collected, an organization must give its customers the opportunity to choose whether to share their sensitive information (e.g., data related to factors such as health, race, or religion).

ONWARD TRANSFER. Unless they have the individual's permission to do otherwise, organizations may share information only with those third parties that belong to the Safe Harbor Agreement or follow its principles.

4 American Institute of Certified Public Accountants, Inc., and Canadian Institute of Chartered Accountants, AICPA/CICA SysTrust Principle and Criteria for Systems Reliability (1999), 3.

5 "A New Covenant with Stakeholders: Managing Privacy as a Competitive Advantage, Privacy Risk Management," KPMG LLP, the U.S. member firm of KPMG International, a Swiss association (2001), 22–23.

SECURITY AND DATA INTEGRITY. Organizations need to ensure that the data they maintain are accurate, complete, and current, and thus reliable for use. They must also ensure the security of the information by protecting it against loss, misuse, unauthorized access, disclosure, alteration, and destruction.

ACCESS. Unless they would be unduly burdened or violate the rights of others, organizations must give individuals "access to personal data about themselves and provide an opportunity to correct, amend, or delete such data."

ENFORCEMENT. Organizations must "enforce compliance, provide recourse for individuals who believe their privacy rights have been violated, and impose sanctions on their employees and agents for non-compliance."

CONTINUOUS AUDITING

Continuous auditing techniques need to be developed that will enable the auditor to review transactions at frequent intervals or as they occur. To be effective, such an approach will need to employ **intelligent control agents** (computer programs) that embody auditor-defined heuristics that search electronic transactions for anomalies. Upon finding unusual events, the control agent will first search for similar events to identify a pattern. If the anomaly cannot be explained, the agent alerts the auditor with an alarm or exception report.

ELECTRONIC AUDIT TRAILS

In an EDI environment, a client's trading partner's computer automatically generates electronic transactions, which are relayed across a **value-added network** (VAN),[6] and the client's computer processes the transactions without human intervention. In such a setting, audits may need to be extended to critical systems of all parties involved in the transactions. Validating EDI transactions may involve the client, its trading partners, and the VAN that connects them. This could take the form of direct review of these systems or collaboration between the auditors of the trading partners and VANs.

CONFIDENTIALITY OF DATA

As system designs become increasingly open to accommodate trading partner transactions, mission-critical information is at risk of being exposed to intruders both from inside and outside the organization. Accountants need to understand the cryptographic techniques used to protect the confidentiality of stored and transmitted data. They need to assess the quality of encryption tools used and the effectiveness of key management procedures that CAs use. Furthermore, the term *mission-critical* defines a set of information that extends beyond the traditional financial concerns of accountants. This broader set demands a more holistic approach to assessing internal controls that ensure the confidentiality of data.

AUTHENTICATION

In traditional systems, the business paper on which it was written determines the authenticity of a sales order from a trading partner or customer. In electronic commerce systems, determining the identity of the customer is not as simple a task. With no physical forms to review and approve, authentication is accomplished through digital signatures and digital certificates. To perform their assurance function, accountants must develop the skill set needed to understand these technologies and their application.

NONREPUDIATION

Accountants are responsible for assessing the accuracy, completeness, and validity of transactions that constitute client sales, accounts receivable, purchases, and liabilities. Transactions that a trading

6 See the appendix for discussion of VANs.

partner can unilaterally repudiate can lead to uncollected revenues or legal action. In traditional systems, signed invoices, sales agreements, and other physical documents provide proof that a transaction occurred. As with the problem of authentication, electronic commerce systems can also use digital signatures and digital certificates to promote nonrepudiation.

DATA INTEGRITY

A nonrepudiated transaction from an authentic trading partner may still be intercepted and rendered inaccurate in a material way. In a paper-based environment, such alterations are easy to detect. Digital transmissions, however, pose much more of a problem. To assess data integrity, accountants must become familiar with the concept of computing a digest of a document and the role of digital signatures in data transmissions.

ACCESS CONTROLS

Controls need to be in place that prevent or detect unauthorized access to an organization's information system. Organizations whose systems are connected to the Internet are at greatest risk from outside intruders. Accounting firms need to be expert in assessing their clients' access controls. Many firms are now performing penetration tests, designed to assess the adequacy of their clients' access control by imitating known techniques that hackers and crackers use.

A CHANGING LEGAL ENVIRONMENT

Accountants have traditionally served their clients by assessing risk (both business and legal) and devising techniques to mitigate and control risk. This risk-assessment role is greatly expanded by Internet commerce, whose legal framework is still evolving in a business environment fraught with new and unforeseen risks. To estimate a client's exposure to legal liability in this setting, the public accountant must understand the potential legal implications (both domestic and international) of transactions that the client's electronic commerce system processes. For example, a web page from which customers order goods opens the organization to national and international business communities and exposes it to multiple and possibly conflicting legal statutes. Legal issues relating to taxes, privacy, security, intellectual property rights, and libel create new challenges for the accounting profession, which must provide its clients with rapid and accurate advice on a wide range of legal questions.

Summary

This chapter focused on Internet commerce, including business-to-consumer and business-to-business relationships. Internet commerce has been the source of intense interest because it enables thousands of business enterprises of all sizes and millions of consumers to congregate and participate in worldwide commerce. The chapter examined Internet technologies, including packet switching, the World Wide Web, Internet addressing, and protocols. Several advantages of Internet commerce were reviewed, including access to worldwide markets, reductions in inventory, creation of business partnerships, reductions in prices, and better customer service.

Electronic commerce is also associated with unique risks. The primary concerns intranets pose (discussed in the appendix) come from employees. Internet risks were characterized as a number of specific fraud schemes that threaten consumer privacy and the security of transmitted and stored data. Several measures were examined that can reduce risks and promote an environment of security and trust. These include data encryption, digital certificates, firewalls, and third-party trust seals for websites.

The chapter concluded with a review of implications for accountants and the profession. The issues covered included privacy issues, continuous process auditing, electronic audit trails, and the auditors' need for new skill sets to deal with highly technical, evidential matter that redefine traditional auditing concerns.

Appendix

Intra-organizational Electronic Commerce

Distributed data processing was introduced in Chapter 1 as an alternative to the centralized model. Most modern organizations use some form of distributed processing to process their transactions; some companies process all of their transactions in this way. Organizations that own or lease networks for internal business use intranets. The following section examines several intranet topologies and techniques for network control.

Network Topologies

A network topology is the physical arrangement of the components (e.g., nodes, servers, communications links) of the network. In this section, we examine the features of five basic network topologies: star, hierarchical, ring, bus, and client-server. Most networks are a variation on, or combination of, these basic models. However, before proceeding, working definitions are presented for some of the terms that will be used in the following sections.

LOCAL AREA NETWORKS AND WIDE AREA NETWORKS

One way of distinguishing between networks is the geographic area that their distributed sites cover. Networks are usually classified as either local area networks (LANs) or wide area networks (WANs). LANs are often confined to a single room in a building, or they may link several buildings within a close geographic area. However, a LAN can cover distances of several miles and connect hundreds of users. The computers connected to a LAN are called nodes.

When networks exceed the geographic limitations of the LAN, they are called WANs. Because of the distances involved and the high cost of telecommunication infrastructure (telephone lines and microwave channels), WANs are often commercial networks (at least in part) that the organization leases. The nodes of a WAN may include microcomputer workstations, minicomputers, mainframes, and LANs. The WAN may be used to link geographically dispersed segments of a single organization or connect multiple organizations in a trading partner arrangement.

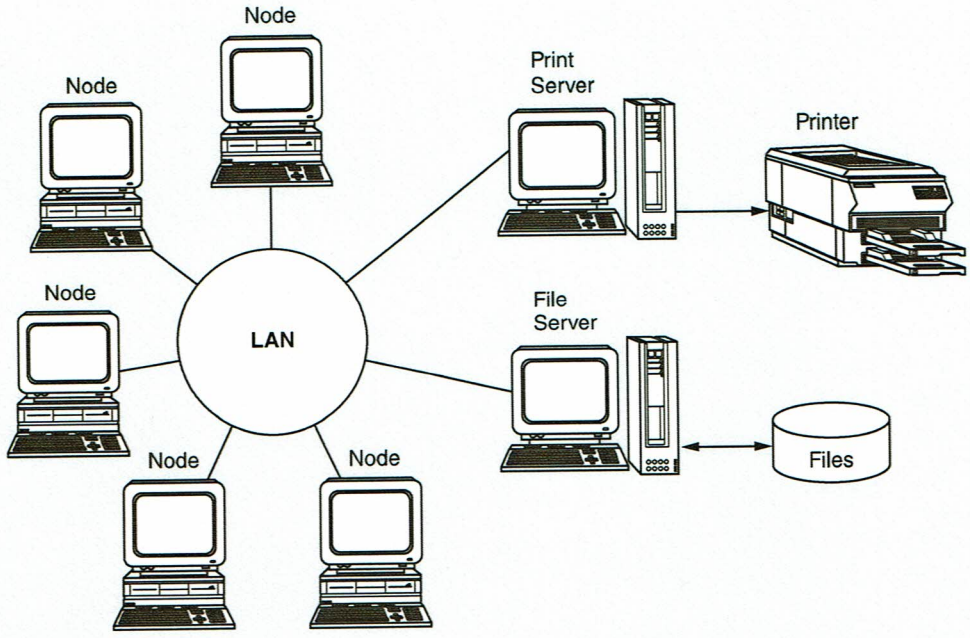
NETWORK INTERFACE CARDS

The physical connection of workstations to the LAN is achieved through a network interface card (NIC), which fits into one of the expansion slots in the microcomputer. This device provides the electronic circuitry needed for internode communications. The NIC works with the network control program to send and receive messages, programs, and files across the network.

SERVERS

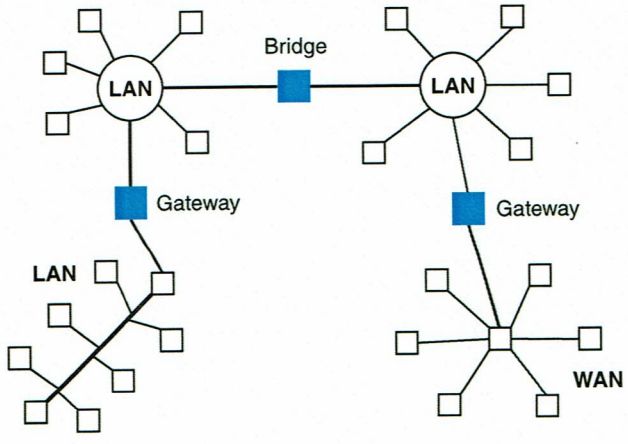
LAN nodes often share common resources such as programs, data, and printers, which are managed through special-purpose computers called servers, as depicted in Figure 12-6. When the server receives requests for resources, the requests are placed in a queue and are processed in sequence.

FIGURE 12-6 LAN WITH FILE AND PRINT SERVERS



In a distributed environment, there is often a need to link networks. For example, users of one LAN may share data with users on a different LAN. Networks are linked via combinations of hardware and software devices called bridges and gateways. Figure 12-7 illustrates this technique. Bridges provide a means for linking LANs of the same type, for example, an IBM token ring to another IBM token ring. Gateways connect LANs of different types and are also used to link LANs to WANs. With these definitions in mind, we now turn our attention to the five basic network topologies.

FIGURE 12-7 BRIDGES AND GATEWAYS LINKING LANS AND WANS



STAR TOPOLOGY

The star topology shown in Figure 12-8 describes a network of computers with a large central computer (the host) at the hub that has direct connections to a periphery of smaller computers. Communications between the nodes in the star are managed and controlled from the host site.

The star topology is often used for a WAN, in which the central computer is a mainframe. The nodes of the star may be microcomputer workstations, minicomputers, mainframes, or a combination. Databases under this approach may be distributed or centralized. A common model is to partition local data to the nodes and centralize the common data. For example, consider a department store chain that issues its own credit cards. Each node represents a store in a different metropolitan area. In Figure 12-8, these are Dallas, St. Louis, Topeka, and Tulsa. The nodes maintain local databases, such as records for customers holding credit cards issued in their areas and records of local inventory levels. The central site—Kansas City—maintains data common to the entire regional area, including data for customer billing, accounts receivable maintenance, and overall inventory control. Each local node is itself a LAN, with point-of-sales (POS) terminals connected to a minicomputer at the store.

If one or more nodes in a star network fail, communication between the remaining nodes is still possible through the central site. However, if the central site fails, individual nodes can function locally, but cannot communicate with the other nodes.

Transaction processing in this type of configuration could proceed as follows. Sales are processed in real time at the POS terminals. Local processing includes obtaining credit approval, updating the customer's available credit, updating the inventory records, and recording the transaction in the transaction file (journal). At the end of the business day, the nodes transmit sales and inventory information to the central site in batches. The central site updates the control accounts, prepares customer bills, and determines inventory replenishment for the entire region.

The assumption underlying the star topology is that primary communication will be between the central site and the nodes. However, limited communication between the nodes is possible. For example, assume a customer from Dallas was in Tulsa and made a purchase from the Tulsa store on credit. The Tulsa database would not contain the customer's record, so Tulsa would send the transaction for

FIGURE 12-8 STAR NETWORK

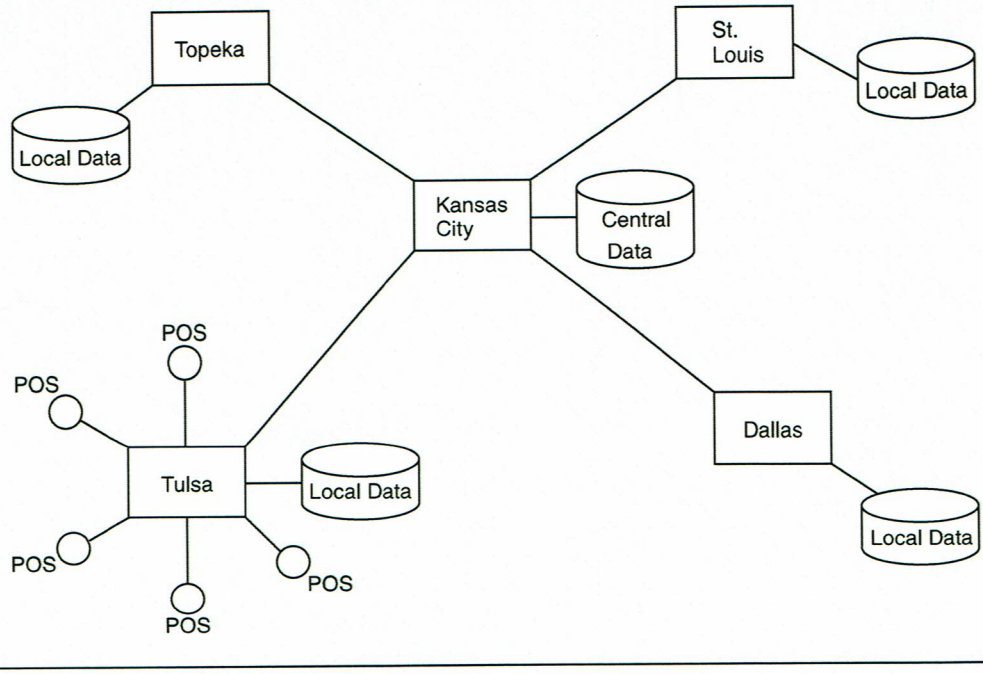
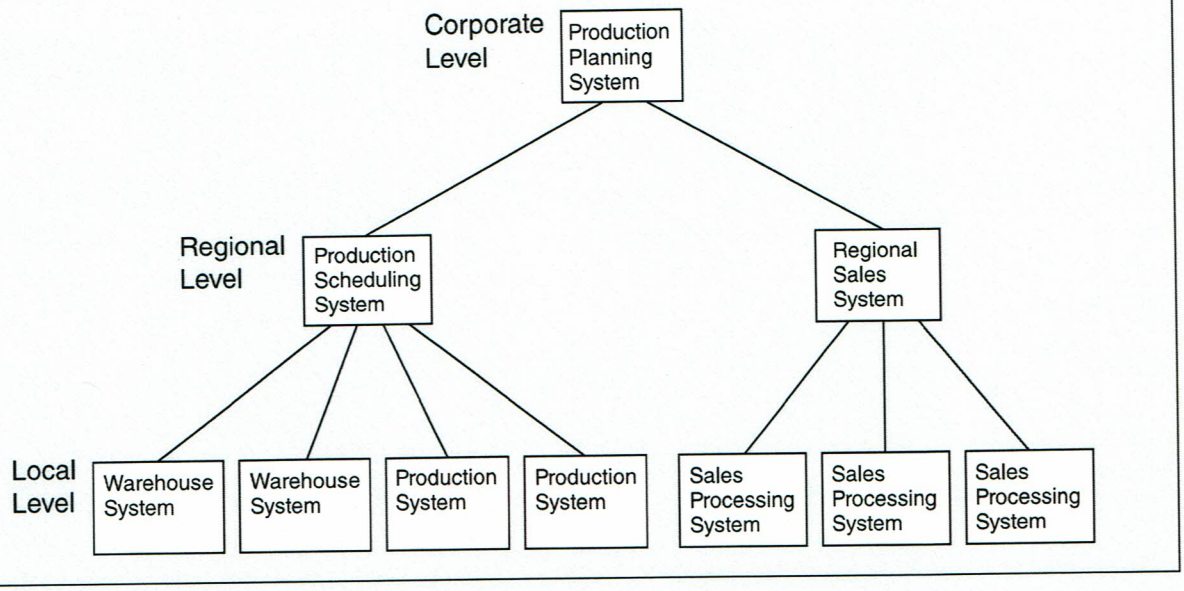


FIGURE 12-9 HIERARCHICAL TOPOLOGY



credit approval to Dallas via Kansas City. Dallas would then return the approved transaction to Tulsa via Kansas City. Inventory and sales journal updates would be performed at Tulsa.

This transaction-processing procedure would differ somewhat depending on the database configuration. For example, if local databases are partial replicas of the central database, credit queries could be made directly from Kansas City. However, this would require keeping the central database current with all the nodes.

HIERARCHICAL TOPOLOGY

A hierarchical topology is one in which a host computer is connected to several levels of subordinate, smaller computers in a master-slave relationship. This structure is applicable to firms with many organizational levels that must be controlled from a central location. For example, consider a manufacturing firm with remote plants, warehouses, and sales offices like the one illustrated in Figure 12-9. Sales orders from the local sales departments are transmitted to the regional level, where they are summarized and uploaded to the corporate level. Sales data, combined with inventory and plant capacity data from manufacturing, are used to compute production requirements for the period, which are downloaded to the regional production scheduling system. At this level, production schedules are prepared and distributed to the local production departments. Information about completed production is uploaded from the production departments to the regional level, where production summaries are prepared and transmitted to the corporate level.

RING TOPOLOGY

The ring topology illustrated in Figure 12-10 eliminates the central site. This is a peer-to-peer arrangement in which all nodes are of equal status; thus, responsibility for managing communications is distributed among the nodes. Every node on the ring has a unique electronic address, which is attached to messages such as an address on an envelope. If Node A wishes to send a message to Node D, then Nodes B and C receive, regenerate, and pass on the message until it arrives at its destination. This is a popular topology for LANs. The peer nodes manage private programs and databases locally. However, a file server that is also a node on the network ring can centralize and manage common resources that all nodes share.

The ring topology may also be used for a WAN, in which case the databases may be partitioned rather than centralized. For example, consider a company with widely separated warehouses, each with