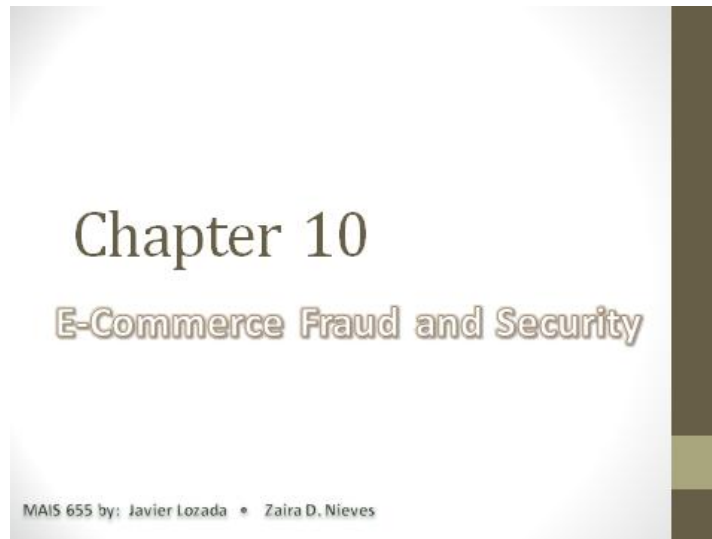


Slide 1



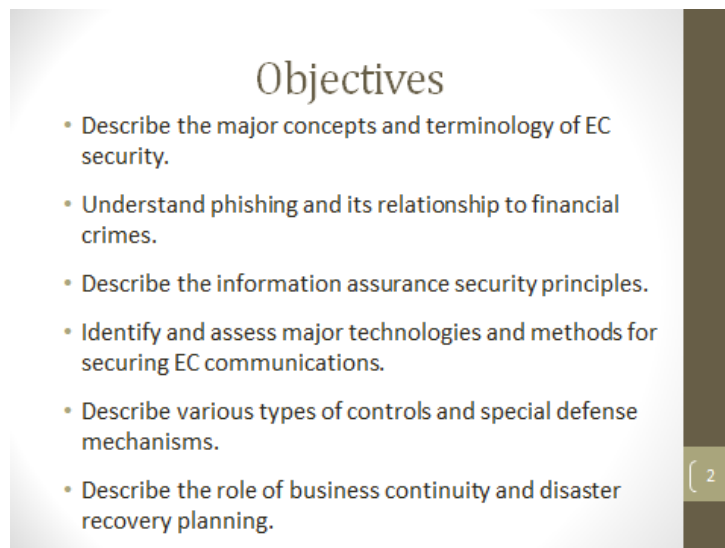
Chapter 10

E-Commerce Fraud and Security

MAIS 655 by: Javier Lozada • Zaira D. Nieves

This slide features a light gray background with a dark brown vertical bar on the right side. The title 'Chapter 10' is centered in a large, dark serif font. Below it, the subtitle 'E-Commerce Fraud and Security' is centered in a smaller, dark sans-serif font. At the bottom left, the text 'MAIS 655 by: Javier Lozada • Zaira D. Nieves' is displayed in a small, dark sans-serif font.

Slide 2



Objectives

- Describe the major concepts and terminology of EC security.
- Understand phishing and its relationship to financial crimes.
- Describe the information assurance security principles.
- Identify and assess major technologies and methods for securing EC communications.
- Describe various types of controls and special defense mechanisms.
- Describe the role of business continuity and disaster recovery planning.

[2]

This slide features a light gray background with a dark brown vertical bar on the right side. The title 'Objectives' is centered in a large, dark serif font. Below it, a bulleted list of six objectives is presented in a dark sans-serif font. At the bottom right, the number '2' is enclosed in square brackets within a small dark box.

The Information Security Problem

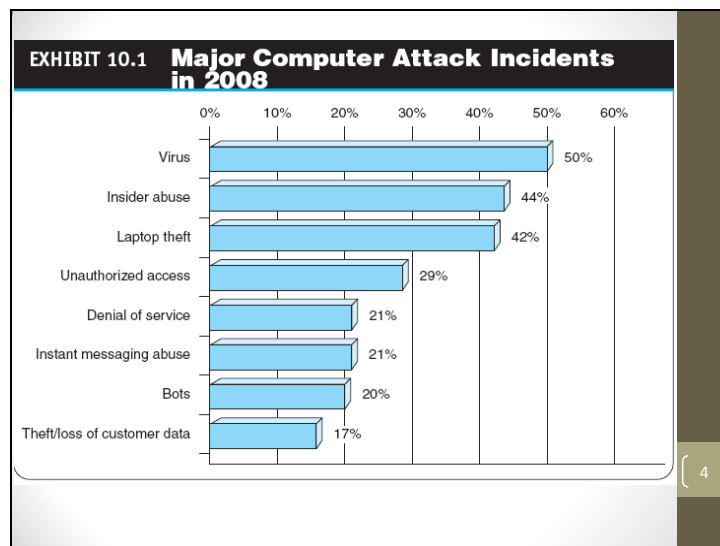
- **WHAT IS EC SECURITY?**
 - Refers to the protection of data, networks, computer programs, computer power and other elements of computerized information systems
- **CSI Computer Crime and Security Survey**
 - Annual security survey of U.S. corporations, government agencies, financial and medical institutions, and universities conducted jointly by the FBI and the Computer Security Institute

{ 3 }

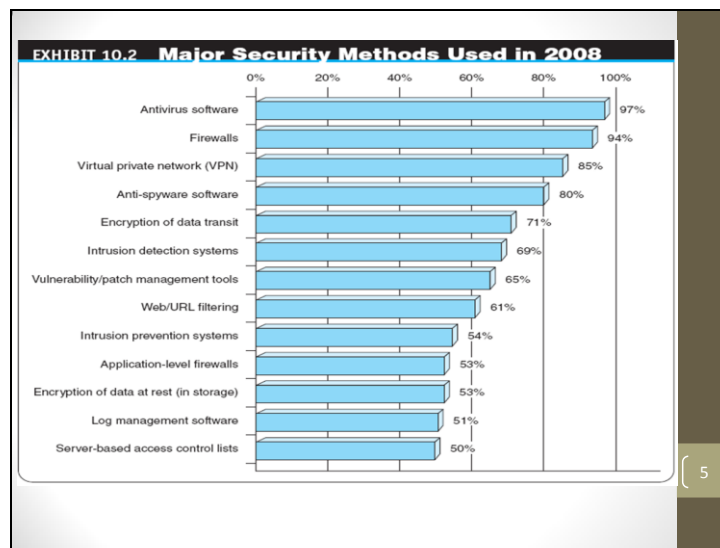
If you examine different list of management concerns regarding the use of EC and IT, the securities issues is and has been among the top concerns. Securing data, transactions, and privacy and protecting people (buyers and sellers) is of utmost importance in conducting EC of any type.

- CSI Computer Crime and Security Survey

No one really knows the true impact on online security breaches because according to the Computer Security Institute (CSI), only 27% of business report to legal authorities about computer intrusions.



Slide 5



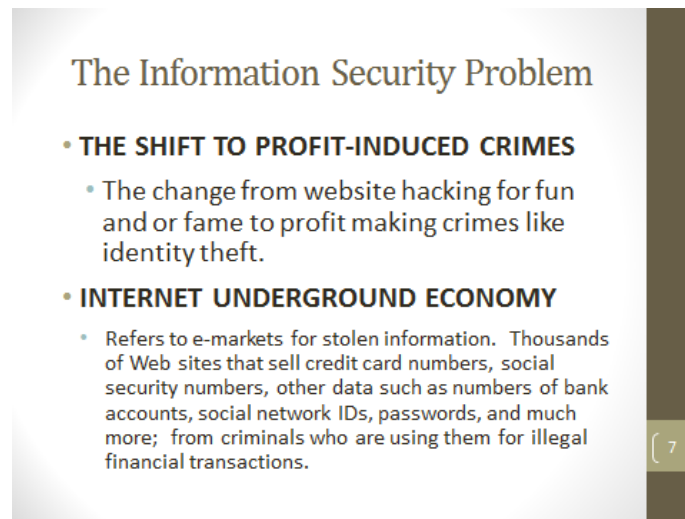
Slide 6

The Information Security Problem

- **THE DRIVERS OF EC SECURITY PROBLEMS**
 - The Internet's Vulnerable Design
 - **domain name system (DNS)**
Translates (converts) domain names to their numeric IP addresses
 - **IP address**
An address that uniquely identifies each computer connected to a network or the Internet

- Security problems are the result of several drivers.
 - The Internet's Vulnerable Design
 - The lack of source authentication and data integrity checking in DNS operations leave nearly all Internet services vulnerable to attacks.
 - The Shift to Profit-Induced Crimes and the underground internet
 - The dynamic nature of EC systems and the role of insiders.

Slide 7



The Information Security Problem

- **THE SHIFT TO PROFIT-INDUCED CRIMES**
 - The change from website hacking for fun and or fame to profit making crimes like identity theft.
- **INTERNET UNDERGROUND ECONOMY**
 - Refers to e-markets for stolen information. Thousands of Web sites that sell credit card numbers, social security numbers, other data such as numbers of bank accounts, social network IDs, passwords, and much more; from criminals who are using them for illegal financial transactions.

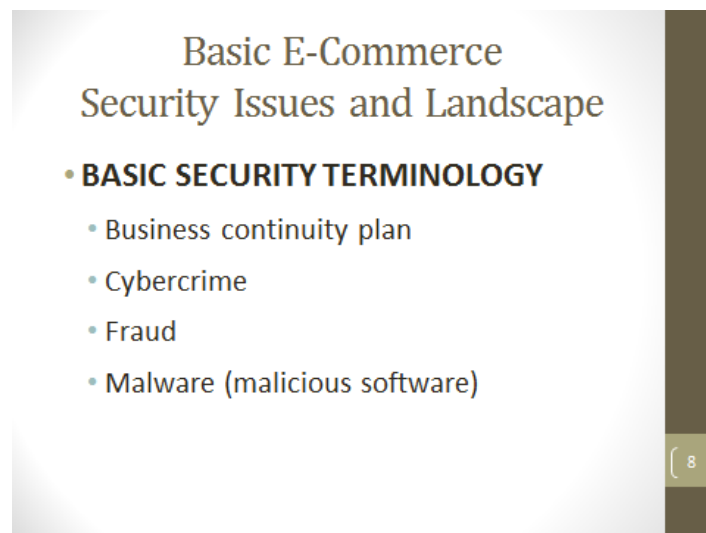
[7]

- **The Shift to Profit-Induced Crimes**

In the early days of e-commerce, many hackers simply wanted to gain fame by defacing Web sites.

Today's criminals are profit-oriented. Most popular is the theft of personal information, such as credit card, bank accounts, etc.

Slide 8



Basic E-Commerce Security Issues and Landscape

- **BASIC SECURITY TERMINOLOGY**
 - Business continuity plan
 - Cybercrime
 - Fraud
 - Malware (malicious software)

[8]

In order to better understand security problem, we need to understand some basic concepts in EC and IT security:

- **business continuity plan**

A plan that keeps the business running after a disaster occurs. Each function in the business should have a valid recovery capability plan

- **cybercrime**
Intentional crimes carried out on the Internet
- **fraud**
Any business activity that uses deceitful practices or devices to deprive another of property or other rights
- **malware (malicious software)**
A generic term for malicious software

Slide 9

Basic E-Commerce Security Issues and Landscape

- Phishing
- Social engineering
- Spam
- Vulnerability
- Zombies



[9]

- **phishing**
A crimeware technique to steal the identity of a target company to get the identities of its customers
- **social engineering**
A type of nontechnical attack that uses some ruse to trick users into revealing information or performing an action that compromises a computer or network
- **spam**
The electronic equivalent of junk mail
- **vulnerability**
Weakness in software or other mechanism that threatens the confidentiality, integrity, or availability of an asset (recall the CIA model). It can be directly used by a hacker to gain access to a system or network
- **zombies**
Computers infected with malware that are under the control of a spammer, hacker, or other criminal

Basic E-Commerce Security Issues and Landscape

- **SECURITY SCENARIOS AND REQUIREMENTS IN E-COMMERCE**
 - EC Security Requirements
 - authentication
 - authorization
 - nonrepudiation



[10]

EC security involves more than just preventing and responding to cyberattacks.

To protect EC transactions we use the following
EC Security Requirements:

- **authentication**
Process to verify (assure) the real identity of an individual, computer, computer program, or EC Web site
- **authorization**
Process of determining what the authenticated entity is allowed to access and what operations it is allowed to perform
- **nonrepudiation**
Assurance that online customers or trading partners cannot falsely deny (repudiate) their purchase or transaction

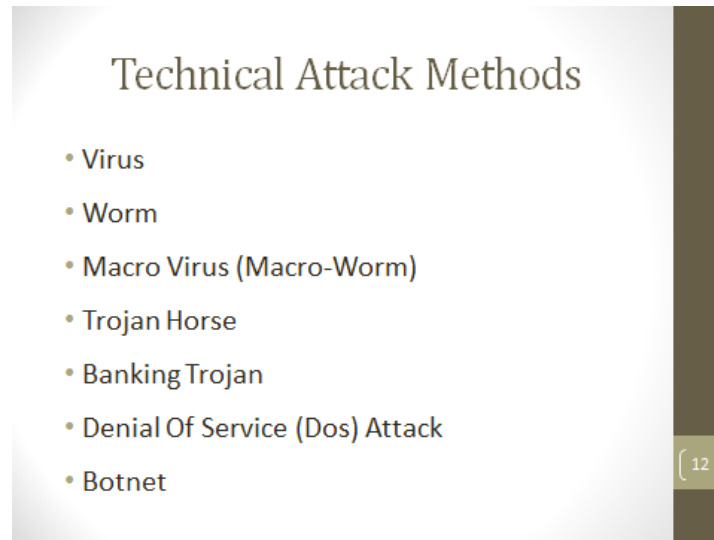
The image shows a presentation slide with a white background and a dark vertical bar on the right. The title is "Basic E-Commerce Security Issues and Landscape". Below it is a section header "THE DEFENSE: DEFENDERS AND THEIR STRATEGY". Underneath are three bullet points: "EC security strategy" (with sub-bullets "Deterring Measures", "Prevention Measures", and "Detection Measures"), and "Information assurance (IA)". A small box with the number "11" is in the bottom right corner of the slide area.

EC Security strategy uses the process of:

- deterring measures
Actions that will make criminals abandon their idea of attacking a specific system (e.g., the possibility of losing a job for insiders)
- prevention measures
Ways to help stop unauthorized users (also known as “intruders”) from accessing any part of the EC system
- detection measures
Ways to determine whether intruders attempted to break into the EC system; whether they were successful; and what they may have done

Making sure that a shopping experience is safe and secure. The ultimate goal in EC security is often referred to as Information assurance (IA):

- **Information assurance (IA)**
The protection of information systems against unauthorized access to or modification of information whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats



- **virus**
A piece of software code that inserts itself into a host, including the operating systems, in order to propagate; it requires that its host program be run to activate it
- **worm**
A software program that runs independently, consuming the resources of its host in order to maintain itself, and that is capable of propagating a complete working version of itself onto another machine
- **macro virus (macroworm)**
A macro virus or macro worm is executed when the application object that contains the macro is opened or a particular procedure is executed
- **Trojan horse**
A program that appears to have a useful function but that contains a hidden function that presents a security risk
- **banking Trojan**
A Trojan that comes to life when computer owners visit one of a number of online banking or e-commerce sites
- **denial of service (DOS) attack**
An attack on a Web site in which an attacker uses specialized software to send a flood of data packets to the target computer with the aim of overloading its resources
- **botnet**
A huge number (e.g., hundreds of thousands) of hijacked Internet computers that have been set up to forward traffic, including spam and viruses, to other computers on the Internet

Phishing, Financial Fraud, and Spam

- **PHISHING**
- **FRAUD ON THE INTERNET**
 - Click fraud
 - Identity theft
 - E-mail spam
 - Search engine spam
 - Spam site
 - Splog
 - Spyware



[13]

- Phishing: in the field of computer security, phishing is the criminal, is the fraudulent process of attempting to acquire confidential information such as user names, passwords and credit card details.
- **FRAUD ON THE INTERNET**
Phishing is the first step that leads to fraud

Types of Fraud:

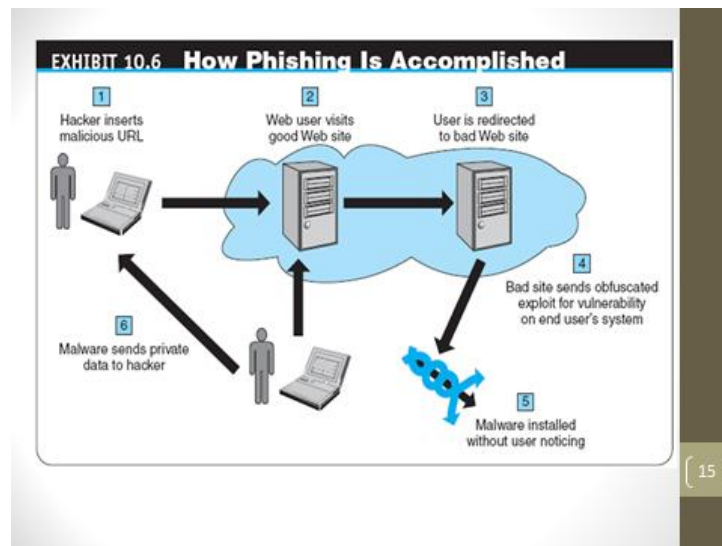
- **click fraud**
Type of fraud that occurs in pay-per-click advertising when a person, automated system, or computer program simulates individual clicks on banner or other online advertising methods
- **identity theft**
Fraud that involves stealing an identity of a person and then the use of that identity by someone pretending to be someone else in order to steal money or get other benefits
- **e-mail spam**
A subset of spam that involves nearly identical messages sent to numerous recipients by e-mail
- **search engine spam**
Pages created deliberately to trick the search engine into offering inappropriate, redundant, or poor quality search results.

- **spam site**
Page that uses techniques that deliberately subvert a search engine's algorithms to artificially inflate the page's rankings
- **splog**
Short for *spam blog sites*. A blog is created solely for marketing purposes. Spammers creates hundreds of splogs that they link to the spammer's site to increase the site search engine rankings.
- **spyware**
Software that gathers user information over an Internet connection without the user's knowledge. Los spywares extend beyond monitoring, can collect various types of personal information such as internet surfing habits and site that have been visited.

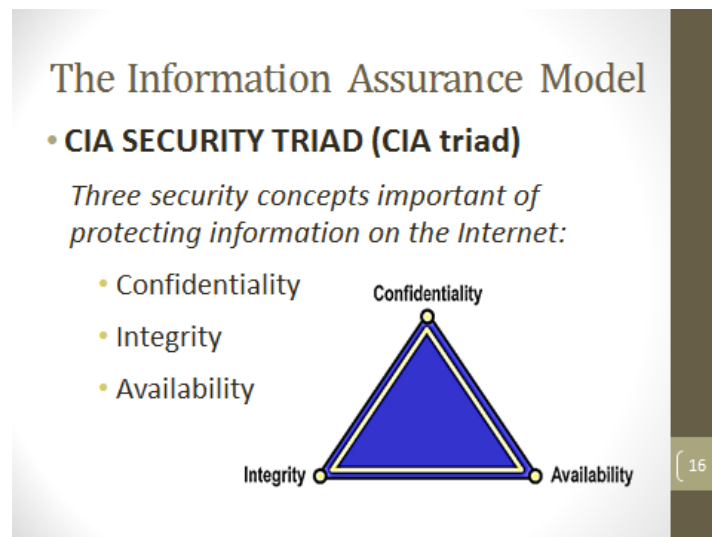
Slide 14



Slide 15



Slide 16

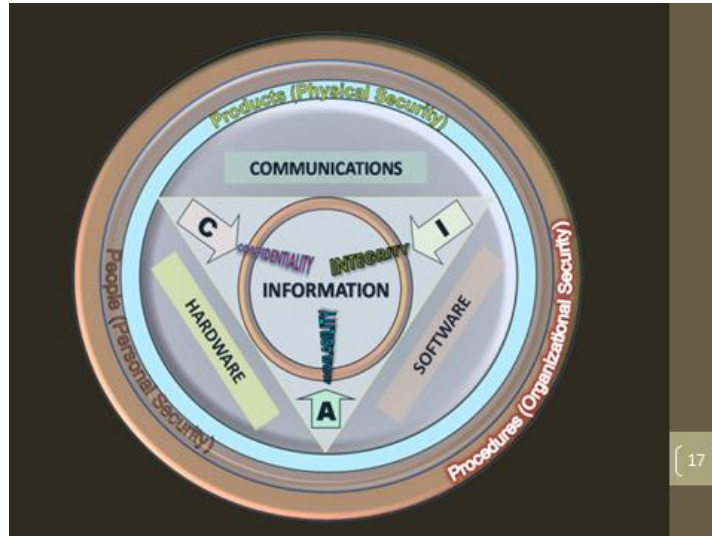


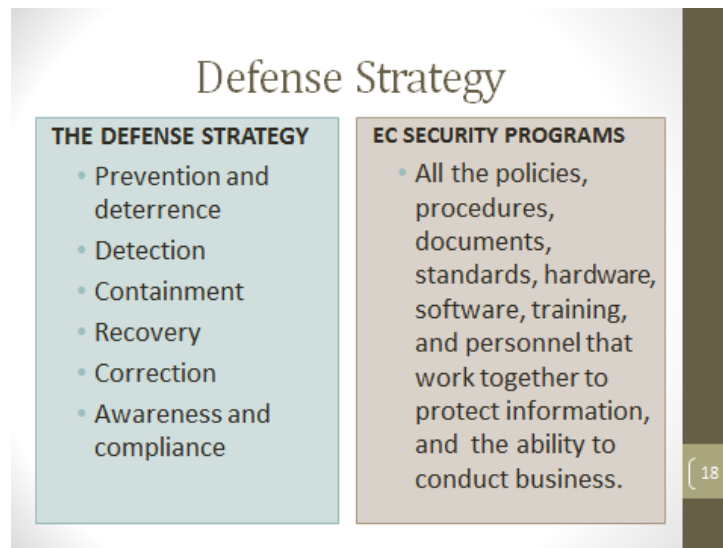
The information assurance (IA) model provides a framework for protection of information system against unauthorized access. The importance of the IA model to EC is that represents the process of protecting information by assuring: confidentiality, integrity, and availability. The model is known as CIA security triad.

- **confidentiality**
Assurance of data privacy and accuracy. Keeping private or sensitive information from being disclosed to unauthorized individuals, entities, or processes

- **integrity**
Assurance that stored data has not been modified without authorization; a message that was sent is the same message that was received
- **availability**
Assurance that access to data, the Web site, or other EC data service is timely, available, reliable, and restricted to unauthorized users

Slide 17





- The defense strategy and control that should be used depend on what needs to be protected.
 - Prevention and deterrence: Properly designs controls may prevent error from occurring, deter criminals from attacking the system, and better yet deny access to unauthorized people.
 - Detection: Detection can be performed by using special diagnostics software's.
 - Containment: (contain damage o damage control) to minimize the loss once malfunction has occurred.
 - Recovery: how to fix a damage information system as quickly as possible.
 - Correction: correcting the causes of damage systems can prevent the problem from occurring again.
 - Awareness and compliance: all organizations members must be educated about the hazards and must comply with the security rules of the organization.
- EC security programs:
 - Have a life cycle, and throughout that life cycle the EC security requirements must be continuously evaluated and adjusted.

The Defense I:
Access Control, Encryption, and PKI

- **ACCESS CONTROL**
 - Passive token
 - Active token
 - Smart cards, chain tokens
 - Biometric control & Biometric systems

19

Access Control

- **passive token**
Storage device (e.g., magnetic strip) that contains a secret code used in a two-factor authentication system
- **active token**
Small, stand-alone electronic device that generates one-time passwords used in a two-factor authentication system
- **biometric control**
An automated method for verifying the identity of a person based on physical or behavioral characteristics
- **biometric systems**
Authentication systems that identify a person by measurement of a biological characteristic, such as fingerprints, iris (eye) patterns, facial features, or voice

The Defense I:
Access Control, Encryption, and PKI

- **ENCRYPTION AND THE ONE-KEY (SYMMETRIC) SYSTEM**
 - Encryption
 - Symmetric (private) key encryption
- **PUBLIC KEY INFRASTRUCTURE (PKI)**

A scheme for securing e-payments using public key encryption and various technical components

 - Public (asymmetric) key encryption

[20]

- ENCRYPTION AND THE ONE-KEY (SYMMETRIC) SYSTEM
 - **encryption**

The process of scrambling (encrypting) a message in such a way that it is difficult, expensive, or time-consuming for an unauthorized person to unscramble (decrypt) it
 - **symmetric (private) key encryption**

An encryption system that uses the same key to encrypt and decrypt the message
- PKI
 - public (asymmetric) key encryption**

Method of encryption that uses a pair of matched keys—a public key to encrypt a message and a private key to decrypt it, or vice versa

 - **public key**

Encryption code that is publicly available to anyone
 - **private key**

Encryption code that is known only to its owner

The Defense I:
Access Control, Encryption, and PKI

- **DIGITAL SIGNATURE OR DIGITAL CERTIFICATE**
 - Hash
 - Message Digest (MD)
 - Digital Envelope
 - Certificate Authorities (Cas)
 - Secure Socket Layer (SSL)
 - Transport Layer Security (TLS)

21

- **Digital signature or digital certificate**

Validates the sender and time stamp of a transaction so it cannot be later claimed that the transaction was unauthorized or invalid.

- **hash**

A mathematical computation that is applied to a message, using a private key, to encrypt the message.

- **message digest (MD)**

A summary of a message, converted into a string of digits after the hash has been applied

- **digital envelope**

The combination of the encrypted original message and the digital signature, using the recipient's public key

- **certificate authorities (CAs)**

Third parties that issue digital certificates. This is a certificate that contains things such as holder's name, validity period, public key information, and signed hash of the certificate data.

- **Secure Socket Layer (SSL)**

Invented by Netscape, is a Protocol that utilizes standard certificates for authentication and data encryption to ensure privacy or confidentiality

- **Transport Layer Security (TLS)**

As of 1996, SSL was renamed to Transport Layer Security

The Defense II:
Securing E-Commerce Networks

- **Firewall**
- **Demilitarized Zone (Dmz)**
- **Virtual Private Network (Vpn)**
- **Intrusion Detection System (Ids)**
- **Honeynet**
 - A network of honeypots
 - Honeypot
 - Penetration test (pen test)

[22]

The major components for protecting internal information flow inside organizations are:

- **Firewall**

A single point between two or more networks where all traffic must pass (choke point); the device authenticates, controls, and logs all traffic
- **Demilitarized zone (DMZ)**

Network area that sits between an organization's internal network and an external network (Internet), providing physical isolation between the two networks that is controlled by rules enforced by a firewall
- **virtual private network (VPN)**

A network that uses the public Internet to carry information but remains private by using encryption to scramble the communications, authentication to ensure that information has not been tampered with, and access control to verify the identity of anyone using the network
- **intrusion detection system (IDS)**

A special category of software that can monitor activity across a network or on a host computer, watch for suspicious activity, and take automated action based on what it sees
- **honeynet**

Is a network of honeypots designed to attract hackers.

 - **honeypot**

are information systems resources like (e.g., firewalls, routers, Web servers, database servers) that looks like production system but do no real work. Acts as a decoy and is watched to study how network intrusions occur

- **application controls**
Controls that are intended to protect specific applications
 - **intelligent agents**
Software applications that have some degree of reactivity, autonomy, and adaptability—as is needed in unpredictable attack situations. An agent is able to adapt itself based on changes occurring in its environment

Slide 25

The Defense III: General Controls and Other Defense Mechanisms

- **PROTECTING AGAINST SPAM**
 - (CAN-SPAM) Act of 2003
 - Protection Against Splogs
- **PROTECTING AGAINST POP-UP ADS**
 - Protection Against Phishing
- **PROTECTING AGAINST SPYWARE**

{ 25 }

The purpose is continuing protecting and preventing.

- **PROTECTING AGAINST SPAM**

Every act to send spam that disguises a sales pitch to look like a personal e-mail to bypass filters violates the **Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003**.

- Law that makes it a crime to send commercial e-mail messages with false or misleading message headers or misleading subject lines

Blog owners can use a **Captcha tool** (Completely Automated Public Turing test to tell Computers and Humans Apart), which uses a verification test on comment pages to stop scripts from posting automatically.

- **PROTECTING AGAINST POP-UP ADS**

Sometimes it is even difficult to close these ads when they appear on the screen. One way to avoid the potential danger lurking behind pop-up ads is to install software that will block pop-up.

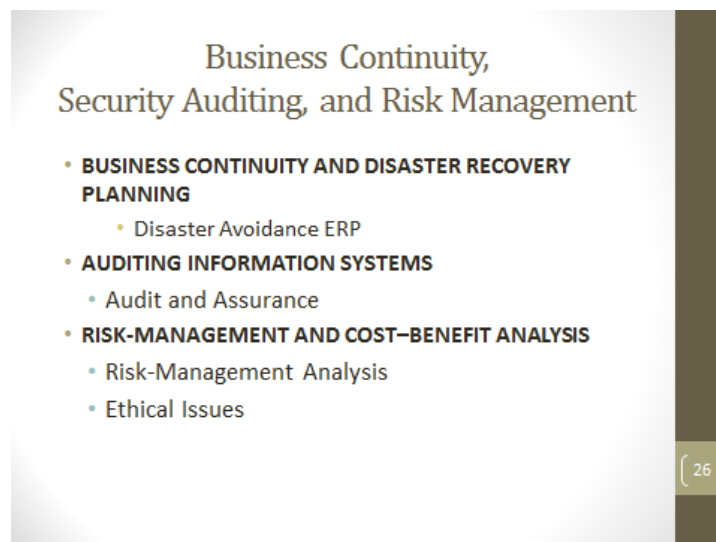
- Protection Against Phishing

Hay varios programas informáticos anti-phishing disponibles. La mayoría de estos programas trabajan identificando contenidos phishing en sitios web y correos electrónicos; algunos software anti-phishing pueden por ejemplo, integrarse con los navegadores web y clientes de correo electrónico como una barra de herramientas que muestra el dominio real del sitio visitado. Los filtros de spam también ayudan a proteger a los usuarios de los phishers, ya que reducen el número de correos electrónicos relacionados con el phishing.

- **PROTECTING AGAINST SPYWARE**

In response to the emerge of spyware, a large variety of anti-spyware software exists. The US Federal Trade Commission has placed on the internet a page of advice to consumers about how to lower the risk of spyware infection.

Slide 26



- **disaster avoidance**

An approach oriented toward prevention. The idea is to minimize the chance of avoidable disasters (such as fire or other human-caused threats)

It is difficult to many organizations to obtain insurance for their computers and information system without showing a satisfactory disaster prevention and recovery plan.

- **audit**
An important part of any control system. Auditing can be viewed as an additional layer of controls or safeguards. It is considered as a deterrent to criminal actions especially for insiders

- **RISK-MANAGEMENT AND COST-BENEFIT ANALYSIS**

It is usually not economical to prepare protection against every possible threat. An IT security program must provide a process for assessing threats and deciding which ones to prepare for and which ones to ignore.

- Risk-Management Analysis
This analysis can be enhance by the use of DSS (Decision Support System) software packages.
- Ethical Issues
Implementing security programs raises several ethical issues. There are ethical and legal obligations that may require companies to “invade privacy” of employees and monitor their actions. In particular, IT security measures are needed to protect against loss, liability, and litigations. Losses are not just financial, but also include the loss of information, customers, trading partners, brand image, and ability to conduct business due to the actions of hackers, malware or employees.

Slide 27

**Implementing Enterprise wide
E-Commerce Security**

- **EC SECURITY POLICIES AND TRAINING**
 - Acceptable use policy (AUP)
- **EC SECURITY PROCEDURES AND ENFORCEMENT**
 - Business impact analysis (BIA)

(27)

The next step is to develop a general EC security policy, as a mention earlier

- **acceptable use policy (AUP)**
Policy that informs users of their responsibilities when using company networks, wireless devices, customer data, and so forth

- **EC SECURITY PROCEDURES AND ENFORCEMENT**

Require an evaluation of the digital and financial assets at risk including cost and operation considerations.

- **business impact analysis (BIA)**

An exercise that determines the impact of losing the support of an EC resource to an organization and establishes the escalation of that loss over time, identifies the minimum resources needed to recover, and prioritizes the recovery of processes and supporting systems

After EC security program and policies are defined and risk assessment completed, the software and hardware can be put in place. Keep in mind that security is an ongoing multilayer process and not a problem that has one solution as is forgotten.

Slide 28

The screenshot shows a CBS News Investigates article from April 4, 2011, at 5:13 PM. The article is titled "Secret Service investigates Epsilon data breach" and is posted by Laura Strickler with 2 comments. The article discusses a data breach at Epsilon, a major email marketing company, which has affected several large corporations including Best Buy, Capital One, JP Morgan Chase, and TVo. The breach involved the compromise of names and email addresses of at least 20 companies, including Kroger, Hilton Honors, Home Shopping Network, and Marriott Rewards. The article also mentions that Epsilon handles email marketing for 2,500 companies and sent 40 billion emails last year. It notes that the breach occurred on March 30th and that the Secret Service is currently investigating the incident. A sidebar on the right contains a "MOST POPULAR" section with five items, including a story about a first lady's close call and another about a woman cut out of a pregnancy. There is also an advertisement for EarthShare.org.

http://www.cbsnews.com/8301-31727_162-20050575-10391695.html



5 Tips For Protecting Against Spam Attacks



[29]

5 Tips For Protecting Against Spam Attacks

1. Watch out for social networking spam
2. Know how to respond properly
3. Don't click on links from emails you can't trust or not solicited
4. Keep your computer operating system and security software up to date
5. Install a dedicated anti-spam application

[30]