Chapter-8
E-Business Security, Privacy, and Legal Requirements

There are several strategies that can help you to reduce the risks by which you and your customers face when doing business online. Be aware of these risks and take steps to deal with them before they become problems.

PROTECTING YOUR CLIENTS

It is important to earn consumer trust online because your customers want to be protected against fraud. Make use of security certifications and encryption technologies that make your website safer to use, and display any accompanying logos signifying that your website is safe. Immediately notify your client of any breaches in security. Your clients want to protect their privacy, so avoid asking them for more information than required. When you send electronic messages to your customers, be sure that you are compliant with the requirements

8.1 SECURITY

Just as you would protect your physical business, you need to ensure the online security of your operations and your customers.

- Get Cyber Safe-Protect your business: Learn how to protect your business and safeguard private information.
- Payment Card Industry Security Standards Council: If you handle debit and credit cards in your business, learn about applying information security best practices.

8.2 INTRANET AND EXTRANET SECURITY SYSTEMS

Fortunately, there are a variety of techniques available to address these security holes within Extranets and Intranets. Before choosing a particular technology, however, it is important to understand the full range of issues that security systems should address:

a. **Authentication**

Ensuring that entities sending messages, receiving messages, or accessing systems are who they say they are, and have the privilege to undertake such actions.

b. **Privacy**

Enabling only the intended recipient to view an encrypted message.

c. **Content Integrity**

Guaranteeing that messages have not been altered by another party since they were sent.

d. **Non-Repudiation**

Establishing the source of a message so that the sender cannot later claim that they did not send the message.

e. **Ease of use**

Ensuring that security systems can be consistently and thoroughly implemented for a wide variety of applications without unduly restricting the ability of individuals or organizations to go about their daily business

8.3 BENEFITS OF THE INTRANET AND EXTRANET

Once up and running, Intranets and Extranets reduce costs and improve operations in many ways, including:

a. **Reducing costs of distributing information**

Intranets make it faster and easier to distribute policies, procedures, and company news to employees; Extranets make it easy and inexpensive to distribute online catalogs and price lists

b. **Lowering administrative costs**

The interactive capabilities of the Intra/Extranet allow users to complete many tasks themselves that once required administrative assistance.

c. **Improving collaboration**

Users become more productive by using the Intra/Extranet to form virtual, online teams. These virtual teams can collaborate without the expense of frequent travel or the delays of sending information via the postal service. Within an organization, the Intranet can flatten hierarchies, giving more employees access to the information they need to make strategic decisions. Extranets allow businesses to collaborate more closely with each other as well. For example, Extranets can be used to integrate the supply chain, replacing expensive and proprietary systems such as electronic data interchange.

8.4 TYPES OF SECURITY RISKS ENCOUNTERED ON AN INTRANET AND EXTRANET

Intranet and Extranet security breaches can take a variety of forms. For example,

- An unauthorized person, such as a contractor or visitor, might gain access to a company's computer system.
- An employee or supplier authorized to use the system for one purpose might use it for another. For example, an engineer might break into the HR database to obtain confidential salary information.
- Confidential information might be intercepted as it is being sent to an authorized user. For example, an intruder might attach a network sniffing device to the network. While sniffers are normally used for network diagnostics, they can also be used to intercept data coming over the wire.
- Users may share documents between geographically separated offices over the Internet or Extranet, or telecommuters accessing the corporate Intranet from their home computer can expose sensitive data as it is sent over the wire.
- Electronic mail can be intercepted in transit.

8.5 FIREWALLS AND THEIR EVOLUTION

A firewall is a network security device that grants or rejects network access to traffic flows between an untrusted zone (e.g., the Internet) and a trusted zone (e.g., a private or corporate network). The firewall acts as the demarcation point or "traffic cop" in the network, as all communication should flow through it and it is where traffic is granted or rejected access. Firewalls enforce access controls through a positive control model, which states that only traffic defined in the firewall policy is allowed onto the network; all other traffic is denied (known as "default deny").

8.6 TYPES OF FIREWALL

PROXY FIREWALL

An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network. However, this also may impact throughput capabilities and the applications they can support.

Stateful inspection firewall

Now thought of as a “traditional” firewall, a stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules as well as context, which refer to using information from previous connections and packets belonging to the same connection.

Unified threat management (UTM) firewall

A UTM device typically combines, in a loosely coupled way, the functions of a stateful inspection firewall with intrusion prevention and antivirus. It may also include additional services and often cloud management. UTMs focus on simplicity and ease of use.

Next-generation firewall (NGFW)

Firewalls have evolved beyond simple packet filtering and stateful inspection. Most companies are deploying next-generation firewalls to block modern threats such as advanced malware and application-layer attacks. According to Gartner, Inc.’s definition, a next-generation firewall must include:

- Standard firewall capabilities like stateful inspection
- Integrated intrusion prevention
- Application awareness and control to see and block risky apps
- Upgrade paths to include future information feeds
- Techniques to address evolving security threats

8.7 COMMON FIREWALL FILTERING TECHNIQUES

Firewalls are used to protect both home and corporate networks. A typical firewall program or hardware device filters all information coming through the Internet to your network or computer system. There are several types of firewall techniques that will prevent potentially harmful information from getting through:

Packet Filter

Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure.

Application Gateway

Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.

Circuit-level Gateway

Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

Proxy Server

Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

In practice, many firewalls use two or more of these techniques in concert. A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted.

8.8 CRYPTOGRAPHY

Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Cryptography concerns itself with the following four objectives:

1) **Confidentiality** -the information cannot be understood by anyone for whom it was unintended.

2) **Integrity** -the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected

3) **Non-repudiation** -the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information

4) **Authentication** -the sender and receiver can confirm each other's identity and the origin/destination of the information.

8.9 DIGITAL SIGNATURE

Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message. Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party. Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer. In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.

8.10 VIRTUAL PRIVATE NETWORK (VPN)

A VPN or Virtual Private Network is a network connection that enables you to create a secure connection over the public Internet to private networks at a remote location. With a VPN, all network traffic (data, voice, and video) goes through a secure virtual tunnel between the host device (client) and the VPN provider's servers, and is encrypted. VPN technology uses a combination of features such as encryption, tunnelling protocols, data encapsulation, and certified connections to provide you with a secure connection to private networks and to protect your identity.

VPN connections technically give you all the benefits of a Local Area Network (LAN), which is similar to that found in many offices but without requiring a hard-wired connection. Early VPNs were often set up to give individual employees secure remote access to their company networks, hence the name "virtual private network". By connecting to the company's network, an individual employee can access all the company's resources and services as if the employee were inside the company. Since then, VPNs have evolved to provide the same level of secure communication between any device on the internet. Today, using VPN is increasingly popular among consumers as a means to protect their privacy online, secure their browsing sessions, and get unrestricted access to content or websites that are otherwise blocked or censored.

8.11 TYPES OF VPN

VPNs differ by architecture, purpose of usage, and accessibility. Two basic types of accessibility are **site-to-site VPN** and **remote access VPN**.

Site-to-site VPNs are used in the corporate environment. A site-to-site VPN ensures the safe encrypted connection of two or more local area networks (LANs) of the same company or of different companies. It means two geographically separated offices are virtually bridged together into a single LAN and users can access data throughout this network.

Remote Access VPNs connect an individual computer to a private network. This type of VPN can be divided again into two groups:

- Corporate VPNs

  Corporate VPNs allow business travellers and telecommuters to connect to their company networks and remotely access resources and services on the networks. When a user connects his/her device to the company's VPN, the VPN thinks that the user's computer is on the same local network as the VPN.

- Personal VPNs

  Personal VPNs provide consumers with the same private and secure connection as the corporate VPNs. However, personal VPNs are not used to connect to private networks to access private resources.

Security is an essential part of any transaction that takes place over the internet. Customer will lose his/her faith in e-business if its security is compromised. Following are the essential requirements for safe e-payments/transactions

Confidential

Information should not be accessible to unauthorized person. It should not be intercepted during transmission.

Integrity

Information should not be altered during its transmission over the network.

Availability

Information should be available wherever and whenever requirement within time limit specified.

Authenticity

There should be a mechanism to authenticate user before giving him/her access to required information.

Non-Repudiability

It is protection against denial of order or denial of payment. Once a sender sends a message, the sender should not able to deny sending the message. Similarly the recipient of message should not be able to deny receipt.

Encryption
Information should be encrypted and decrypted only by authorized user.

Auditability
Data should be recorded in such a way that it can be audited for integrity requirements.

8.12 MEASURES TO ENSURE SECURITY

Major security measures are following:-

Encryption
It is a very effective and practical way to safeguard the data being transmitted over the network. Sender of the information encrypt the data using a secret code and specified receiver only can decrypt the data using the same or different secret code.

Digital Signature
Digital signature ensures the authenticity of the information. A digital signature is a e-signature authenticated through encryption and password.

Security Certificates
Security certificate is unique digital id used to verify identity of an individual website or user.

Important Points:

- A firewall is a network security device that grants or rejects network access to traffic flows between an untrusted zone (e.g., the Internet) and a trusted zone (e.g., a private or corporate network)
- The proxy server effectively hides the true network addresses.
- Cryptography is closely related to the disciplines of cryptology and cryptanalysis
- Digital signatures are the public-key primitives of message authentication.
- Cryptography concerns with Confidentiality, Integrity, Non-repudiation and Authentication
- A VPN or Virtual Private Network is a network connection that enables you to create a secure connection over the public Internet to private networks at a remote location.

- Security certificate is unique digital id used to verify identity of an individual website or user.

Practice Questions

Objective type questions:

Q1. Essential requirements for safe E-payment
a. Confidential
b. Integrity
c. Authenticity
d. All of these

Q2. UTM Stands for
a. Universal threat management
b. Unified threat management
c. Unified threshold management
d. None

Q3. NGFW stands for
a. New-general firewall
b. Next-general firewall
c. Next-generation firewall
d. None

Very short answer type questions:

Q1. Define Digital Signature.
Q2. Define Intranet.
Q3. Define Content Integrity.
Q4. Define Privacy.
Q5. What is the use of Proxy Server?
Q6. What is the full form HTTP?

Short answer type questions:

Q1.What is the purpose of Encryption?
Q2. Why security is required in E-commerce?
Q3. What is Extranet and it's use?
Q4. What is Authentication?
Q5. What is the use of proxy firewall?
Q6 What is Cryptography?

Essay type questions:

Q1. What is VPN ? Explain it's type.
Q2. What is Firewall ? Explain it's uses.
Q3. Explain Firewall filtering techniques.
Q4. Explain the benefits of Extranet and Intranet.

Answers key for objective questions

Q1: d
Q2: b
Q3: c