UNIT

2 Security Threats to E-Commerce

Q. 1. Give some Security threats to E-Commerce.

Ans. Most businesses that have made the move towards an online presence have experienced some kind of security threat to their business. Since the internet is public system in which every transaction can be tracked, logged, monitored and stored in many locations. It is important for business to understand possible security threats for their business.

There are many threats to E-commerce that may come from sources with an organization or through some external channel. The following are the top corporate security threats categorized by internal and external threats:

1. Unauthorized internal users who access confidential information by using a stolen password for the purpose of committing fraud or theft.
2. Weak access point in information infrastructure and security that can expose company information and trade threat.
3. Management that underline security is maybe the greatest risk to e-commerce.
4. Contractors, partners, Consultants, etc. who take advantage of even limited access to important system.
5. People's mentality on the Internet Security is changing, this is evident through the increase in sales of antivirus software.

Q. 2. Explain the term E-Cash?

Ans. E-Cash is a computer generated Internet based system which allow funds to be transferred and items to be purchased by credit cards, cheque or by money order, providing secure on-line transaction processing. While many different companies are rushing to offer digital money product, currently E-cash is represented by two models: -

1. One is the **On-line** form of e-cash which allow for the completion of all type of internet transactions.
2. The other form is **Off-line;** essentially a digitally encoded card that could be used for many of the same transaction as cash.
   - The primary function of e-cash is to facilitate transaction on the internet.
   - The reality of e-cash is only slightly more complicated, and these complications make the transaction both secure and private.
   - E-cash truly globalize the economy, since the user can download money into his/her cyber wallet in any currency desired.
   - To the extent a user want e-cash offline all that is necessary is smart card technology.
   - It is similar to debit/ credit card, but e-cash allow individual to conduct transaction with each other.
   - It is similar to personal cheque, but it is feasible for very small transaction.

Q. 3. Write a short note on:

(A) Debit Card

(B) Credit Card

ANS. Debit Card: A Debit card is a plastic card that provides an alternative payment method to cash when making purchase.

- It can be called an electronic cheque, as the funds are withdrawn directly from either from the bank account, or from the remaining balance on the card.
- In some cases, the cards are designed exclusively for use on the internet, and so there is no physical card.
- Like Credit cards, Debit cards are used widely for telephone and Internet purchase and, unlike credit cards, the funds are transferred immediately from the bearer's bank account instead of having bearer pay back the money at a later date.
- Debit cards may also allow for instant withdrawal of cash, aching as the ATM card.
- There are currently three ways that debit cards transactions are processed: -
  (a) Online Debit
  (b) Offline Debit
  (c) Electronic Purse card system

Advantage: For most transactions, a debit card can be used to void cheque writing altogether.

Disadvantage: Use of debit card is not usually limited to the existing fund in the account to which it is linked, most bank allow a certain threshold over the available bank balance.

Credit Cards:

- Credit Cards are small plastic cards issued to user as a system of payment.
- It allows its holder to buy goods and services based on the holder's promise to pay for these goods and services.
- The user of the e-card creates a revolving account and grants a line of credit to the consumer from which the user can borrow money for payment to a merchant.
- The credit card is different from a charge card.
- **The ability to obtain credit is both a blessing and a curse**
- It allows you to fund big purchases when you are short of money, giving you the option to pay them off over a period of time.
- However, you must be disciplined and not spend beyond your need.
- If you plan to borrow using your credit card, you also need to understand the term and in particular the way interest charges are computed.

Q. 4. Explain the concept in electronic payment system.

Ans. Electronic payment are the central part of e-commerce activities as it deals with the strategies for the payments of goods and services by online customers. Electronic payment system implies cryptography. The original purpose of cryptography was to hide something that had been written.

- Cryptography can be used to hide the meaning of information in any form, such as data stored on a disk or message in transit through a communication network.

- When electronic payments are sent through a network the biggest risk is that payment message might be altered and the risk that someone reads the message may be of a minor significance.
- The process of checking the integrity of the transmitted message is often called message authentication. The most recent and useful development in the uses of cryptography is the **digital signature.**
- It can prevent fraud in electronic commerce and assure the validity of financial transaction.

Q. 5. What do you understand by virtual organization; Write the characteristics of a virtual organization.

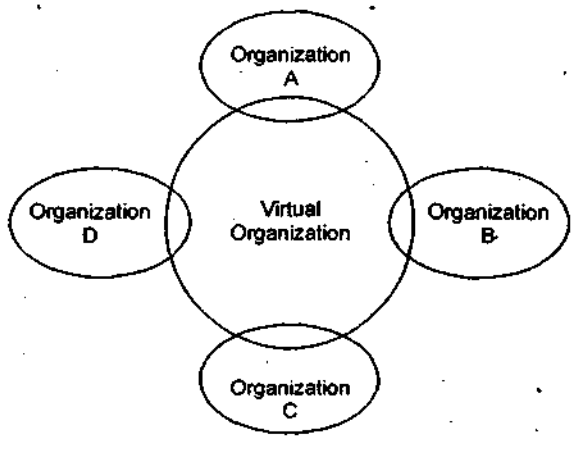
or

What is Virtual Organization?

Ans. The term Virtual organization is used to describe a network of independent firms that join together, often temporarily, to produce a service or product. Virtual organization is often associated with terms as virtual office, virtual terms and virtual leadership. The ultimate goal of virtual organization is to provide innovative, high quality products and services instantaneously in response to customer demands.

- Virtual Organizations are distributed "business processes". The processes may be owned by one or more organizations acting in partnership, for a specific project, resources are assembled to perform a business process on behalf of the project owner, and then disassembled on the completion of the contract.
- Virtual organization is a geographically distributed organization whose members are bonded by a long term common interest or goal.

A virtual organization is an organization existing as a corporate, not for profit, educational or otherwise productive entity that otherwise does not have a central geographical location and exist through telecommunication tools.



Virtual Organization

Example: A small software company wants to bid for a new contract, which is beyond its scope. This company forms a VO with other similar small companies and by doing that it is suddenly able to compare with larger Corporations to gain the contract.

Characteristics of a Virtual Organization: Virtual organizations can be large or small, long or short lived. Other characteristics of virtual organizations are:

- VO exists for a specific purpose.
- VO does quickly deliver products/ services that are innovative and customized.
- Membership and structure of a VO evolve over time.
- VO members can switch from one project to another.
- Dynamic VOs have a capability to unite quickly.
- Resources, services and people that comprise a VO can be single or multi-institutional homogeneous or heterogeneous.
- **Principle of Synergy (many to one):** VO exhibits unifying property because it is constituted from different organizational entities that create an effect of single organization.
- **Principle of Divergence (one-to-many):** A single organization can exhibit multiplication property by participating in many VOs at the same time.

Advantages/ Benefits of VO:

1. VOs make it possible to satisfy constantly changing customer and market requirements in a competitive manner.
2. An ability to participate in VOs increases the service range a company can offer its customers.
3. Participation in VOs increases the total number of end-customers a company can reach indirectly via its partners.
4. It become possible to provide services precisely tailored to a specific customer need.

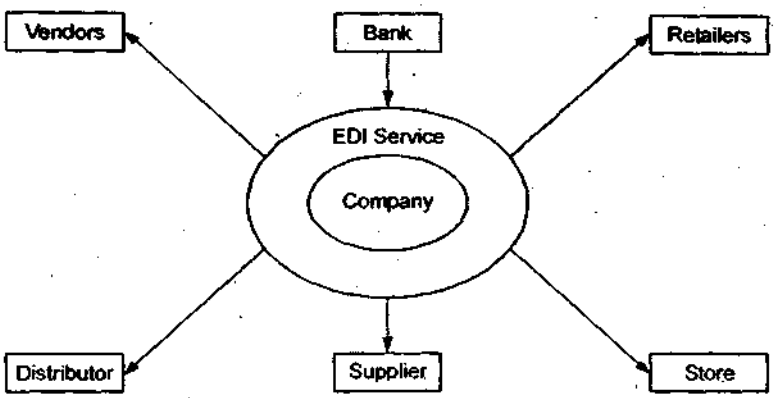
Disadvantages/ Drawbacks of VO:

1. **High Cost:** The main costs are related to investment and subsequently high operational costs, including training and maintenance.
2. **Legal Problems:** VOs are established fast and efficiently to respond to market opportunities or tackle specific projects. This can result in complex legal problems as the boundaries between the organizations becomes vague or fluid.
3. **Trust and respect issues:** Trust and respect are one of the most important factors for a successful VO. This applies both for knowledge sharing and the group dynamics for collaboration.
4. **Cultural Issues:** Co-operation in VOs may involve working across culture. This is a big challenge to many managers, and requires them to transfer their business policies and culture to work with dispersed business teams spanning organization geography, and cultures.

Q. 6. What is Electronic Data Interchange (EDI)? Also, give its benefits.

Ans. Electronic Data Interchange: It refers to the computer to computer exchange of structural business information in a standard electronic format. Using EDI, the various trading partners can establish links between their computers to exchange information electronically.

EDI may also be defines as the transfer of structure data between the computers on manually agreed formats known as.EDI formats. The information stored in the source computer in an organization is converted into EI format by software or program and it is received by the recipient computer system for direct usage.



The above diagram shows, a company and its various partner companies like as vendors, banks, retailers, distributors, suppliers and warehouses.

Benefits of EDI: The main advantage of EDI are over the traditional methods of electronic communication using Fax, e-mail etc. are as follows:

1. The information or data sent by one company's computer may be directly used by the recipient's computer without manual intervention.
2. Since standard formats are used for information or data exchanges between the computer systems, of both organizations; it eliminates the data entry errors to a considerable extent.
3. It improves the business cycle of both organizations by providing a link for electronic communication between them.
4. EDI may be used for communication between more than two companies.

5) Instant delivery f information or data on the prescribed digital formats.

Q. 7. What is physical security? Explain the need of physical security.

Ans. Physical Security protects the facilities housing system resource, the system resource themselves and the facilities used to support their operation. Physical Security, as it pertain to computer security, should cover the following area at a minimum: access control, fire safety, failure of supporting utilities, structural collapse and portable system.

Need for the Physical Security:

1. **Physical access to the facility:**
   - Is there any perimeter control for protecting against access? Is it regularly monitored or tested?
   - Does the access control exist to all 'entry point' to the facilities? Is it effective?
   - Are visitors always accompanied? To what extent is the system controlling the access of authorized visitors operating satisfactorily?.
   - Is there a potential for use of online terminal?
2. **Site location:**
   - Is the installation of the site sufficiently away from potential public hazards such as:
   - Gas main and/ or other pipelines.
   - River on low lying areas subject to flooding.

- Other hazards such as oil storage tank, corrosive material.
- Is the location vulnerable to terrorist attacks?
- Is the location on a flight path, that is, proximity to an airport?

3. **Power and Air conditioning mechanisms: -**
   - Is switch-over to backup electric supply automatic without loss of power?
   - Have backup electrical arrangements been tested regularly.
   - Is electric equipment adequate to avoid voltage fluctuation?
   - Are there comprehensive instructions or procedures to be followed in the event of power interruptions?
4. **Fire:**
   - Are the heat and smoke detection linked to security and fire services?
   - Are all areas kept free of combustible material?
   - Are detailed fire instructions displayed and made known to the staff working at the facility?
5. **Natural Disasters:**
   - Have all flood risk been evaluate before developing the facility.
   - Has consideration been given to the possibility of flooding from burst water pipes, washroom, overflow etc?

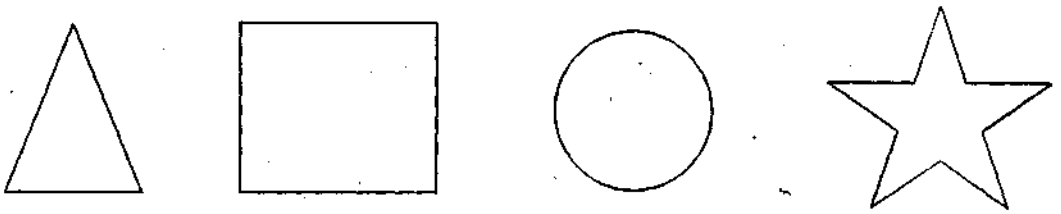
Q. 8. Mention the Natural disaster and control of the physical security and explain them.

Ans. The important factors that are enemies to the physical security of information system resources are:

1. **Fire:** Conflagration caused by fire affect IS through heat, smoke or suppression agent damage.
   - This threat category may be minor, major or catastrophic.

   Control: Install smoke detector near equipments, keep fire extinguisher near equipment and train employees in their proper use and conduct regular fire evacuation exercise.

The fire categories are:



Ordinary combustible **Flammable liquid** **Electrical equipment** **Combustible material**

2. **Environmental Failure:** This is a type of disaster that includes any interruption in the supply of controlled environmental support provided to the operation centre.
   - Environment controls include clean air, air conditioning, humidity and water control: Since human and computer do not exist well, it is good to keep them separate.

- I is essential to keep all rooms containing computer at reasonable temperature (60-75 degree F).

3. **Earthquake:** Earthquake is nothing but a violent ground motion that result from stresses and movement of the earth's surface.
   Control: Keep computer system away from glass and elevated surface, and in high risk areas.
4. **Liquid Leakage:** In spite of best of care taken, small accident can happen in the hand of individual working at office premises and data centre.
5. **Lightening:** An electrical charge of air can cause either direct lightening strike to the facilities, transformers and substations.
   Control: There is a need to install surge suppressions, install and test uninterruptible power supply.

Q. 9. Discuss the fundamental principles of physical security?

or

Give the highlight on the basic tenets of physical security of IS?

Ans. the fundamental principles of the physical security are: -

1. **Defence in depth:** It means deploying multiple measures that complement and support one another. These multiple measure are meant to control: -
   (i) Information system security procedure
   (ii) Physical space
   (iii) Personnel
   - The main physical defence are those nearest the protected information

   The precautions needed for the 'defence-in-depth' are:
   (a) Physical access control measure
   (b) Security alarm system
   (c) Delay unauthorized entry.
2. **Controlling the physical Access:** The number of physical access point at facilities that store or handle information facilities, should be commensurate with safety aspect and work function at the site.
   Access point should have physical security control such as:
   (i) Security doors
   (ii) Shutter
   (iii) Grills
3. **Intrusion detection System:** IDS are designed to detect actual or attempted unauthorized entry, identify its location and signal a response with an alarm. IDS can: -
   (i) Provide continuous surveillance over secure area.
   (ii) Extend coverage into area not usually accessible to guard.
4. **Physical access on a 'Need-to-know' basis:**
   - Access to information system resource must always provide only on a need-to-know basis.
   - The physical measure may be complemented by procedural and personnel measure such as:
     (i) Education and training program.
     (ii) A personnel security system that ensure appropriate approval.

Q. 10. What is meant by Biometrics data? Explain with illustrative examples.

Ans. The term biometrics come from a Greek word **Bios** meaning life and **Metrikos** meaning measure.

- It is well known that the human intuitively uses some body characteristics such as face, voice etc. to recognize each other.
- Biometrics is used as one of the method for physical access control.
- Biometric is a collection of method for identification based on measuring time physiological characteristics that are unique to each and every individual.
- Dome examples of such characteristics are:
  1. Voice
  2. Finger prints
  3. Boy contour
  4. Retina
  5. Hand writing style

Biometrics data have characteristics which are so unique to a person and embedded with a person that it cannot be lost, stolen and copied. Given the unique nature of human biometrics ID, biometrics methods occupy an important place in user identification/authentication.

Q. 11. What are the benefits of biometrics?

Ans. Traditionally passwords and ID cards have been used to restrict access to secure system but these methods can easily be breached and are unreliable.

- Biometric cannot be borrowed, stolen or forgotten and forging one is practically impossible.
- From the preceding discussion, one can see that biometric is an alternative to using passwords for authentication in logical control.
- Biometric is based on the third type of authentication mechanism.
- Biometric is defined as automated means of identifying or authenticating the ID of a living person based on physiological or behavioral characteristic.
- In biometric, identification is a 'one-to -many' search of an individual characteristic from the database of stored image.
- Biometric provide a number of benefits compared to the traditional method.

1. Increase the level of security
2. Greater convenience
3. Higher level of accountability
4. Fraud detection.

Q. 12. What are the criteria used while selecting a Biometric system?

or

What are the criteria used while selecting a biometric characteristic to design a biometric system?

Ans. Biometric is a physical or biological feature or attribute that can be measured. It can be used as a means of providing without revealing your ID that you have a certain right or password.

- We know the critical difference is that biometric is something that is part of you, rather than something you know or can carry with you
- Examples of physiological biometrics feature include height, weight, body odor, the shape of the hands, the pattern of veins, retina, the face and the pattern on the skin of thumb.
- Example of behavioral biometrics are voice pattern, signature and keystroke sequence.
- Most biometric applications are based on certain biometric information.
- Each of the various biometric techniques that exit has its own limitation.

Criteria for selection of Biometric Characteristics:

The Characteristics	The Meaning
1. Universality	1. All the human beings have same physical characterisdics.
2. Uniqueness	2. For human, these characteristics are unique and thus constitute a distinguish feature.
3. Permanence	3. These characteristics remain 'persistent'.
4. Performance	4. The degree of accuracy of identification must be quite high before the system can be operational.
5. Acceptability	5. Application will not be successful if the public offer strong biometric.

Q. 13. How the biometric systems are designed?

Ans. Biometric systems, by their very nature, are complex system with responsive decision making involved in term of physical access controls. The two most critical issues that designers of biometric system face are:

1. Storage and protection of the template.
2. Accuracy of biometric system step.

Storage and Protection of the template: Biometric systems have to scan, store/retrieve a template and match. It is important to note that depending on the design of the system, the match is to be performed in different locations. There can be three different 'modes of protection' that may be used for the template: no protection, data encryption or digital signature.

Accuracy of biometric system step: The evaluation of a biometric system has to be based on the evaluation of all components: the recognition system performance communication interface, the matching and decision and other key factors such as each to use **acquisition** speed and **processing** speed.

Q. 14. Comment on the statement "Legal challenges of Biometrics".

Ans. Government are beginning to mandate that biometric identifiers such as facial images and finger prints should be used in official documents, including passports, Biometrics is also seen as essential for the provision of e-government services to citizen to ensure accurate authentication to prevent fraud. In spite of the current progress in biometric research, legal challenges continue to restrict the use of biometric technologies by both public institution and business. The most pressing legal challenges are in the area of conforming to privacy and data protection requirement.

Q. 15. Give some social issues of the biometric system.

Ans. The main social issues are:

1. **Clarity of purpose:** - It is important to clear about what the needs of application are and how biometric will be able to achieve them.
2. **Interoperability and equivalence of performance and process:** - Process equivalence is extremely important as it impact on system performance, especially where bio-metric are used international situations (e.g. border control IS).
3. **Human Factor engineering, usability and social exclusion:** - Human factor such as age, ethnicity, gender, disease ought to be studied on a case-by-case basis so as to minimize the possibility of social exclusion of a small but significant part of the population.
4. **Element of Trust:** People may temporarily accept to trade in part of their personal freedom in exchange for a more secure world.