E-Commerce Contracts & Risks

BY
Prof. ZAVERI JYOTINDRA

email j.zaveri@dnserp.com
www.dnserp.com

E-Commerce Contract (1)

How you should structure your contract formation for online transactions?

- 1. Establish the offer and acceptance procedure, this must be laid out in the terms and conditions and basically should have an offer made by the customer on the website and acceptance by the retailer.
  - Receipt of payment from a customers' card does not constitute acceptance.

- 2. Completion of order form, should include delivery details, quantity of goods etc. Also it is important to include a submit button, cancel button and as a result of the new E-commerce regulations a clear button so as to allow the customer to correct any errors that they may make.

- 3. Incorporating the terms and conditions, there a few considerations here: firstly a check box should be included to indicate the customer has read and understood the terms and conditions before the 'accept' button can be clicked, also the accept button should not be useable until the page has fully loaded.

E-Commerce Contract – (2) (continued)

- 4. Acknowledging receipt of order, after the card details are validated the E-commerce regulations require that an acknowledgement page is shown to the customer and an acknowledgement email sent.

- For further studies:
- http://www.netlitigation.com/netlitigation/ecommerce.htm

E-Commerce perspectives

- Risks in E-Commerce:
  - Business Risks
  - Information Risks
  - Technology Risks
- In order to minimize security threats, e-commerce firms must develop a reliable corporate policy that takes into account the nature of the RISKS, the information assets that need protecting, and the procedures and technologies required to address the risk, as well as implementation and auditing mechanisms.

Risk Assessment

- A security plan begins with risk assessment
  - An assessment of the risks and points of weakness (vulnerability).
  - To take stock of information assets and knowledge assets of the e-commerce website.
  - What information is at risk? Is it customer's information, proprietary designs, business activities, secret knowhow, or other internal confidential information such as costing, salary data?
  - Try to give value to each – how much it will cost to company if this information is leaked out?

Next is security policy

- Based on your quantified list of risks, you can start to develop a security policy.
  - A set of statements prioritizing the information risks, identifying acceptable risk targets, and identifying the mechanisms for achieving these targets.
  - Who generates and controls this sensitive information in the firm?
  - Plan adequate security measures to protect these information assets.

Secured Electronic Transactions (SET)

- IAM – Identity and Access Management
  - The security organizations generally administers access controls. Authentication and authorization is important.
  - Log in id and secret password is given to users
- Sometime biometrics devices are used along with digital signatures to verify physical attributes associated with an individual, such as fingerprint or retina (eye) scan or speech recognition system.

E-Learning

- Learning using computers is e-learning
  - CD-ROM / DVD based e-learning
  - Web-based learning
- EXAMPLES
  - **http://elearning.nic.in/**
  - **www.gurukulonline.co.in**
  - **http://elearning-india.com/**

E-Learning: Benefits

1. Provides immediate access to training
2. No training lag time for new employees
3. Deliver new product training on time
4. Reduces delivery costs per course
5. Get more value from the training budget
6. Provide training to more people
7. Gives employees more time to do their job
8.   Reduce travel-related travel
9. Delivers training with greater consistency
10. Anywhere / Anytime training

THANK YOU

PRESENTATION BY

JYOTINDRA ZAVERI

email j.zaveri@dnserp.com

www.dnserp.com