The article explains the factors affecting online trust and gives recommendations to improve online trust in emerging economies like India.

Factors affecting Online Trust
As shown in the figure, there are several factors that affect online trust in some way. The signs indicate if a factor has a positive or negative effect on trust.

Following section illustrates how different websites are trying to improve online trust with the help of above factors. In case of certain sites some factors are more important than others in building trust.

Good Online Experience
No one will trust an online e-business vendor, if the person finds it difficult to navigate the site. Bad web experience signals online retailer is not serious about his business. Not having an organized footer design that includes all important links will decrease company’s reputation & trust with customers. A good Example of footer is shown in the snapshot below. (www.bhphotovideo.com) It disseminates important security and privacy information which helps in building elements of trust.
Depth and Quality of Information

Website with good depth and quality of information reduces search cost. It offers customers diverse choices and education about products to make more informed decisions. It results into frequent visits to the site and hence increased customer loyalty. For example Chenneionline.com site has wealth of information about Chennai which ranges from events in city, movies, news, shopping, and health centers to temples and tourist destinations.

Security

Customers are getting more aware about security related terms like SSL certificate, Security bridges provided by third parties. Therefore, they demand these certificates and bridges to be assure of site’s security.

Use of a dedicated SSL certificate
Many online banking sites and email providers use encrypted technology to protect customer data. This type of visual assurance helps online vendors to increase trust and build revenue. Example: Gmail, Onlinesbi use 128 bit encryption to encrypt data. They have their website identities, verified by Thawte SGC CA and VeriSign respectively. (Exhibit2)

Use of Security Badges
Many SSL certificate providers offer badges that customers can click to confirm that the site uses standard encryption. Some companies even sign up for McAfee or Controlscan, which also offer site testing measures.
Building Trust in Online Environment
Thursday, 13 October 2011 13:46

Example: Makemytrip

On clicking Verisign symbol in Onlinesbi.com, we got the verisign assurance certificate as shown in exhibit3. Research shows that McAfee SECURE increases online sales by an average of 12% if the seal is prominently displayed.[i]Example: WholesaleKeychain.com

Privacy Statements
Privacy statement shows commitment of website providers to respect customer’s privacy. Having good privacy policy goes a long way to enhance online trust. Privacy policy mainly consists of following information.

Word of Mouth

Word of mouth, spread through individual experiences, can have a powerful influence on the level of trust consumers have in vendors. Many companies are trying to improve their brand in social media place. They provide social media icons in footer section.

Role of Third Party Players
Third-parties provide independent recommendations on the trustworthiness of vendors. They may come in many forms, from individual recommendations to privacy and security trust “seals” to media representatives/watchdogs.

Watchdogs
These are independent organizations, centers or media representatives that identify vendors’ violations or breeches of trust. They also publicize their actions to alert consumers.

EPIC (Electronic Privacy Information Center) and CDT (Center of Democracy and Technology)
act as privacy watchdogs that continuously monitor the privacy practices of online vendors and provide a forum for consumers to communicate their privacy concerns[ii]

Some third parties also try to create awareness among consumers about online safety and privacy. Examples: http://www.staysafeonline.org/http://www.onguardonline.gov/

Certificate Authorities
Most cryptographic protocols for secure electronic transactions require the presence of a trusted third party, such as a bank or certificate authority (CA). The CA verifies the link between the identities of individuals or vendors and their corresponding public keys, through the use of digital certificates. The CA does not vouch for the trustworthiness of the vendor, but simply authenticates the vendor's identity. Examples are: VeriSign (http://www.verisign.com) and Entrust (http://www.entrust.com/)

Seals of Approval
Third parties also provide seals of approval to assure consumers that a vendor’s site is a reliable and credible place to do business.

Vendors that display a privacy seal convey a message to consumers that they openly disclose and adhere to certain standards for conducting business, and that this disclosure/adherence is assured by a credible third-party regulator. Example: BBBOnline reliability seal

Recommendations for developing countries

Continually growing online infrastructure will help to increase the e-commerce diffusion in India and emerging countries where online business models are taking shapes. This will also increase the problems associated with lack of online trust. In this context, developing countries can learn from steps already taken by developed countries.
Building Trust in Online Environment
Thursday, 13 October 2011 13:46

As shown in the figure, customers feel comfortable to reveal their personal data when the environment is secure i.e. there is a strong policy in place. For instance, when a website has a legally mandated policy, customers are more likely to provide their contact, financial and biological information than a website governed by a moderate policy. This is clearly seen in the market. People are very apprehensive about disclosing their financial and contact information during an e-commerce transaction when the site is not regulated by any legal or strong policy. So strong regulations and standards build trust in the online e-commerce market.

Role of International Laws
If e-commerce is to be a close substitute for normal “bricks-and-mortar” shopping, Web shoppers should be able to expect an equivalent level of protection to other consumers. To a degree, this can be assured through enforcement of existing consumer protection law and practices, and through modification of existing laws and practices as necessary to accommodate the unique characteristics of the online market. This solution is adequate, however, only when all parties to a transaction are located within countries with strong legal protections for consumers. However, when parties to an e-commerce transaction can be individuals located on opposite sides of the globe, traditional “bricks-and-mortar” dispute resolution — e.g. taking one’s case to small claims court — is often impractical.

Role of Private Players
In order to handle this cross-border disputes and often conflicting laws in different countries, developing countries can learn from the example OECD committee. A committee having members from OECD countries has developed Guidelines for Consumer Protection in the Context of Electronic Commerce under the consensus of Member countries. Since e-commerce is truly a global business, developing countries can (and should) be part of these global groups to resolve cross border issues. Private sector companies like Online Mediators, eResolution, and SquareTrade feature online complaint forms and third-party mediators who employ e-mail and organized case-development processes to mediate disputes between parties. Similar mediators in developing countries should be encouraged through government intervention if possible.

Protection of Privacy and Private Data
1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data should be enforced with same vigor as they are followed in developed countries. Businesses should clearly communicate in their privacy statements what kind of info will be collected and how it will be used. This will mitigate the perceived risk of online business. However, self-regulated enforcement with the help of third parties prominent in developed countries won’t work in developing countries. Hence the role of Government has to be proactive to tackle the challenges in e-business by formulating rules and regulations which are governed by an organization that is under the aegis of third party agencies acting in coalescence with the Govt. Third party agencies like OTA can be taken as a benchmark for coming up with a governing and enforcement agency.

Importance of Educating Customers
Role of Govt and private player alliances
In developed countries, some third parties (for example http://www.staysafeonline.org/ http://www.onguardonline.gov/) try to create awareness among consumers, with the help of government, about online safety and privacy. On similar lines, developing country like India should try to create awareness among its citizens.

Role of Ecommerce Business
Ecommerce business should try to educate customers about the advantages of transacting online. In India, Caratlane.com has taken a step in this direction. It educates customers about product features and advantages of buying them online. It helps to increase online diffusion and to make consumers take better decisions.

The framework gives a pictorial idea of how developing countries like India can improve the trust by adopting three-pronged strategy. It has to educate consumers about different online best practices, gain knowledge from the developed countries by participating in different meetings, and committees. Finally, an alliance between Indian government and third parties will help in fostering trust. It will function as an independent privacy watchdog for India which will formulate and enforce different regulations.

Exhibit 1: Snapshot of bad web interface
Exhibit 2: Different encryption technologies used by Gmail and SBI
Exhibit 3: Verisign certificate used by onlineSBI

References

This article has been authored by Nitin Bandgar from IIM Bangalore.