International Journal of Advance and Applied Research
www.ijaar.co.in
ISSN – 2347-7075 Impact Factor – 7.328
Peer Reviewed Bi-Monthly
Vol. 11 No. 5 May-June 2024

Emerging Trends and Challenges in IT Sector

Rahul J Ingawale
Lal Bahadur Shastri College of Arts, Science & Commerce, Satara
Corresponding Author: Rahul J Ingawale
Email: ingawalelibrarian@gmail.com

DOI- 10.5281/zenodo.12228705

Abstract:

The field of Strategic Management is still in its stage of infancy and it has been a couple of decades since this field has been explored on the concepts promoted by none other than Michael Porter. Porter's work is relevant because he built up on the economic theory to produce a frame work for strategy formulation that has proven effective and durable. Porter also has demonstrated that his models apply to Internet-Information related markets and his frameworks clearly provide valuable insights to any industry.

We are aware of some basic dynamics of competition in emerging markets but how to compete in markets very few have known. We also need to know how characteristics of demand and supply affect competition in these markets. In today's business environment most organizations face is how to develop an e-business strategy. For this the development and implementation of **IIOS** [**Internet based Inter-Organizational Systems**] is the need of the hour as these systems appear to have greatest weight. Improvisation in this sector remains among top 10 issues facing IS Executives and Managers.

As e-business strategies have received growing attention from entrepreneurs, executives, investors and the industry, there is a need to develop a successful e-strategy.

IIOS Provides a positive business direction for Internet based IS applications, trading partners, and help in solving technical as well as non-technical issues. Integration of organizational and inter-organizational processes with capabilities to enhance linkages between various trading organizations in Supply Chain and management.

The participants in the process may have complex business relationships, especially between the firms and trading partners, end resulting in a number of social and political factors that influence IIOS Planning and Implementation.

The study of innovation has tremendous potential and the most common question which comes to mind is:
How can firms compete through innovation in Global Markets?

Key Words: Strategic Management, IIOS, Strategic Management, Innovation, IS.

Objective:

- The objective of this paper is to give an outline about the various facets of e-commerce activities taking place across the globe.
- In addition to this, introduction of new and innovative programs to promote better products and services in the field of Internet Advertising and Marketing.
- While the e-commerce activities take place world wide, the hurdles faced by corporate, advertisers, the hosts, consumers etc, are put forth with the best possible solutions available.
- Listing of the legal angles applicable and their importance world wide, taking into consideration of all the aspects which are needed while advertising and marketing through the Internet as the media.
- Insights on the Cyber crimes taking place across the globe and remedial measures to control them.
- Information on the applications of the Laws of the land, The IT Act 2000, with the amendments of 2008 in the era of globalization and competition.

  IIOS would definitely help in achieving diverse objectives and performance outcomes within the context of different trading relationships. Implementation of IIOS requires joint efforts across firm boundaries and the benefits of adopting IIOS are contingent on the status of network adoption by other firms in the trading community.

IIOS implementation reflects in:

1. Change in the structure of the industry and alter the rules of competition.
2. IIOS may enable companies / firms to conduct e-transactions with any business partners in B2B chain.
3. Creation of opportunities to establish interactive relationships among business partners in B2B and B2C.
4. Improvisation in Customer Service and strengthen Back-Office integration.

5. Creation of competitive advantages by providing new avenues and opportunities to cooperate and compete with their competitors.
6. Creation of new business avenues within the company's existing business line.

FTC Compliance Guidelines concerning Internet Advertising and Affiliate Marketing

In an attempt to address consumer privacy interests, the Federal Trade Commission ("FTC") on December 1st 2010, raised concerns that despite industry self-regulatory measures, many marketers either do not disclose their data practices or disclose them in an unintelligible manner. FTC Chairman Jon Leibowitz said,

FTC Guidelines concerning Children's Online Privacy Protection Act [COPPA]

The FTC also has sought details on the review of its Children's Online Privacy Protection Act (COPPA) Rule. COPPA imposes requirements on operators of Web sites that are aimed at children under 13, or that knowingly collect personal information from children under 13, for example, the rule requires online operators to get parental permission before collecting, using, or disclosing personal information from children.

Advertising & Communications Litigation:

The more successful an advertising campaign becomes, the more likely the increased exposure could ultimately lead to a lawsuit. The fact of the matter is, when marketing of a product or service is legally challenged, the reputation of the products and services is also put on the line as well.

In many cases, an advertising dispute is best resolved outside of court by an industry self-regulator. These are often less expensive and less formal, and in many cases work faster than the courts.

There are often conflicts that result from the overlap of marketing and intellectual property. These can be closely related to social networking sites, keyword advertising, and domain names. With the power to police branding and trade-marking issues during application, costly court litigation can be avoided.

These issues can often become conflated with copyright violation and trademarks. Internet marketing is often surrounded in legal gray areas.

New Privacy Policy:

A New Private Policy should be in place as there is a generalized opinion that nothing is private when information is disclosed on the Internet.

The Face book privacy policy has grown from 1,004 words in 2005 to 5,830 today. Face book user now needs to click through more than 50 privacy buttons with more than 170 options in order to opt out of full disclosure of his or her personal information. Face book's privacy policy word count not only has eclipsed the US Constitution, it has also passed other major social networks such as Flickr (384 words), Twitter (1,203), Fraudster (1,977), and MySpace (2,290).

Security Measures:

A state of computer "security" is the conceptual ideal, attained by the use of the three processes:

1. Prevention, 2. Detection, 3. Response.

User account access controls and cryptography can protect systems files and data, respectively.

Firewalls are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering.

Intrusion Detection Systems (IDS's) are designed to detect network attacks in progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.

"Response" is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of legal authorities, counter-attacks, and the like. In some special cases, a complete destruction of the compromised system is favored.

Today, computer security comprises mainly "preventive" measures, like firewalls or an Exit Procedure. Firewalls are common amongst machines that are permanently connected to the Internet (though not universal, as demonstrated by the large numbers of machines "cracked" by worms like the Code Red worm which would have been protected by a properly-configured firewall). However, relatively few organizations maintain computer systems with effective detection systems, and fewer still have organized response mechanisms in place.

What is the importance of Cyber Law?

Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyber laws are a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives.

Cyber laws are meant to set the definite pattern, some rules and guidelines that defined certain business activities going on through internet legal and certain illegal and hence punishable.

The E-commerce industry carries out its business via transactions and communications done through electronic records. It thus becomes essential that such transactions be made legal.

Cyber law is a generic term, which denotes all aspects, issues and the legal consequences on the Internet, the World Wide Web and cyber space.

India is the 13th nation in the world that has cyber legislation apart from countries like the US, Singapore, France, Malaysia and Japan.

Advantages of It Act 2000:

1. The IT Act 2000, the cyber law of India, gives the legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.
2. The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. Let's have an overview of the law where it takes a firm stand and has got successful in the reason for which it was framed.
3. The IT Act 2000 empowers the government departments to accept filing, creating and retention of official documents in the digital format. The Act also puts forward the proposal for setting up the legal framework essential for the authentication and origin of electronic records / communications through digital signature.
4. The Act legalizes the e-mail and gives it the status of being valid form of carrying out communication in India. This implies that e-mails can be duly produced and approved in a court of law, thus can be a regarded as substantial document to carry out legal proceedings.
5. The Act also talks about implementation of digital signatures and creation of digital records. The Act also provides statutory remedy to the corporate in case the crime against the accused for breaking into their computer systems or network and damaging and copying the data is proven. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.
6. Also the law sets up the Territorial Jurisdiction of the Adjudicating Officers for cyber crimes and the Cyber Regulations Appellate Tribunal.
7. The law has also laid guidelines for providing Internet Services on a license on a non-exclusive basis.
8. The IT Act 2000, though appears to be self sufficient, it takes mixed stand when it comes to many practical situations.

Dis-Advantages of It Act 2000:

1. Internet is a borderless medium; it spreads to every corner of the world where life is possible and hence is the cyber criminal. Then how come is it possible to feel relaxed and secured once this law is enforced in the entire nation??
2. The Act initially was supposed to apply to crimes committed all over the world, but nobody knows how can this be achieved in practice, how to enforce it all over the world at the same time???
3. The law misses out completely the issue of Intellectual Property Rights, and makes no provisions whatsoever for copyrighting, trade marking or patenting of electronic information and data. The law even doesn't talk of the rights and liabilities of domain name holders, the first step of entering into the e-commerce.
4. The law is silent over the regulation of electronic payments gateway and segregates the negotiable instruments from the applicability of the IT Act, which may have major effect on the growth of e-commerce in India. It leads to make the banking and financial sectors irresolute in their stands.
5. The IT Act stays silent on filming anyone's personal actions in public and then distributing it electronically. It holds ISPs (Internet Service Providers) responsible for third party data and information, unless contravention is committed without their knowledge or unless the ISP has undertaken due diligence to prevent the contravention.
6. According to Amendments made in 2008 to the IT Act 2000, now an officer in the rank of Police Inspector is empowered to look up into the investigations and filling of charge sheet when any case related to cyber law takes place. This approach is likely to result in misuse in the context of Corporate India as companies have public offices in the metros and semi-metro cities, which would come within the ambit of "public place" under the Act. As a result, these companies will not be able to escape potential harassment at the hands of the Investigating Officer.

Conclusions:

1. Setting up respective offices in order by way of adequate security systems, Firewalls, and "TRUSTED" Administrators will be beneficial for the companies to restrict employees from committing frauds and frequent checks imposed upon by personnel of Top Management.
2. Top Management of the respective companies should impose restrictions on their employees from having access to public sites during office hours on their personal e-mails. Employees should access mails only from the official IDs provided by the Management.
3. The cyber laws of the country can be regarded as insufficient and insecure enough to provide a strong platform to the country's e-commerce industry for which they were meant.
4. India has failed to keep in pace with the world in this respect, and the consequence is not far enough from our sight; that most of the big customers of India's outsourcing activity have to re-think of carrying out their business in India.

5. If India doesn't want to loose its position and wishes to stay as the world's leader forever in outsourcing market, it needs to take fast but intelligent steps to cover the glaring loopholes of the Act, or else the day is not far when the scenario of India ruling the world's outsourcing market will stay alive in the dreams only as it will be overtaken by its competitors.
6. There is no single organization which can control or set standards in Internet Advertising across the world as there are differences in culture, language, Individual Laws of respective countries.
7. Setting up of an International Body on the lines of WTO, NATO, UNSC etc, to take up cases of organized Cyber Crimes and preventions across the world as in the existing scenario a lot has to be done as there are inadequacies in the current systems.
8. Acceptance to standard norms would be a difficult assignment as there are very less number of countries who have come together with a common agenda.
9. Every individual should follow ethical guidelines laid by the respective Laws of the land.
10. A new private policy should be in place with stringent guidelines [on the lines of FTC], to keep watch on unscrupulous elements from barging and privacy violators.

References & Acknowledgements:

1. King. W.R., "IS Strategic Planning- Information Systems Management", 2000.Journal: Kearns.G.S. "Strategic Information Systems", 2000.
2. Article: Lederer, Mirchandani A.L. – "Search For Strategic Advantage From World Wide Web" -2001.
3. Article: Futla, Dhaliwal F., "Electronic Networking Applications & Policy", 2002.
4. Report: FTC Chairman Leibowitz Jon; "Federal Trade Commission Guidelines", December 2010.
5. Police Manual: "Amendments of 2008 to The IT Act, 2000", Police Inspector, Dr. Tungar Sanjay - Cyber Crime Cell, Pune.