North Asian International Research Journal of Social Science & Humanities

ISSN: 2454-9827 Vol. 4, Issue-2 February-2018

IRJIF: 3.015

Index Copernicus Value: 57.07 UGC Journal No: 48727

SECURITY CONCERNS IN INTERNET MARKETING

***MUKESH KUMAR**

****Research Scholar, Department of Commerce and Business Administration***
L.N.Mithila University, Darbhanga

INTRODUCTION

The rapid growth of Internet has changed human life in every aspect, be it communication, culture, entertainment, education or business. But, perhaps nowhere else the impact of Internet felt as in the business sector. The Internet has the potential to radically change the way businesses interact with their customers. The web frees their customers from their traditional passive role as receivers of marketing communication, gives the much greater control over the information search and acquisition process and allows them to become active participants in the marketing process. Companies are realizing the benefits of the revolutionary interactive media and are reaping its benefits. As more and more marketing activities are taking place on the Internet, various strategic issues are also emerging. These are important not only for growth of business, but also for survival in the long term.

The Internet is leading to a fundamental paradigm shift for mass marketing to personalized marketing database and telecommunications technology make it very easy and cost efficient to mass-market personalized services. Although "mass marketed, personalized service" sounds like an oxymoron, it is not. Personalization on the Internet refers to the ability of customers to receive personalized information (eg., sales advertisements or coupons) or visit a web site with a homepage customized from them. Personalisation crosses the boundaries of two of the marketing Ps, product and promotion, because it has the potential to impact and enhance both. Because personalization is automated and it is at the core of many e-marketing methods, it is deemed important enough to hold its own category.

For e-marketing mix, we can think of six "I's framework that summarises how to IT can impact the marketing function, and hence provides a basis for identifying opportunities and predicting future changes. The

six "I"s shows the levers that are available for the e-marketing manager to pull through the use of IT. It may not be necessary to pull all the levers in every situation. The six I's are:

- Integration
- Interactivity
- Individualism
- Independence of location
- Industry restructuring and
- Intelligence

The point to remember when buying over the Internet is that most countries have exactly the same consumer rights ads you would have if you were buying in a mall. But since the buying procedure is different, there is a need for guidelines regarding consumer protection. For example, the law in the U.K. is quite explicit: Anything you purchase must be of merchantable quality. In other words, it must be safe, free from any defects. Secondly, it must be fit for the purpose for which it was designed. And finally, it must be as described. Unfortunately, any law as in the country like U.K. does not protect Indian consumers. Thus, it becomes all the more important that buyers should be careful while shopping online.

One of the most important strategic issues of e-marketing relates to security of business and commercial transactions. A security threat in terms of Internet has been defined a circumstances, conditions or even with the potential to cause economic hardship of data, denial of service and/fraud, waste and abuse. The biggest hurdle is fraud in online credit card transactions. Data suggest that the fraud in online credit card transactions exceed 100 basis points-a full 1% (some estimates place online credit card fraud at 3%-300 basis points). At 1%, the online fraud rate is still 10 times greater that POS and MOTO rates (Coldwell, 2000). Indeed, the online credit card fraud now comprises nearly half of the all-online chargeback's. Peter Thiel, a Pay Pal founder refers to the "tsunami of fraud" and has expressed fears that it will overwhelm the entire company. The Internet security however, does not seem to be a priority with the Indian Internet companies. On an average, an Indian company spends less than 1% of their funds on security. Various preventive measures like cryptography, encryption programmes, firewalls, and wires and protection of programmes etc. are used for providing security to the data and information collected in the computer. Therefore, it suggested that e-marketing companies should protect their own system and personal data.

SECURITY CONCERNS IN INTERNET MARKETING

For both companies and consumers that participate in online business, security concerns are very important. Many consumers are hesitant to buy items over the internet because they do not trust that their personal information will remain private. Recently, some companies that do business online have been caught giving away or selling information about their customers. Several of these companies have guarantees on their websites, claiming customer information will be private. By selling customer information, these companies are breaking their own, publicized policy. Some companies that buy customer information offer the option for individuals to have their information removed from the database (known as opting out). However, many customers are unaware that their information is being shared and are unable to stop the transfer of their information between companies.

Security concerns are of great importance and online companies have been working hard to create solutions. Encryption is one of the main methods for dealing with privacy and security concerns on the Internet. Encryption is defined as the conversion of data into a form called cipher. This cipher cannot be easily intercepted unless an individual is authorized by the program or company that completed the encryption. In general, the stronger the cipher, the better protected the data is. However, the stronger the cipher, the more expensive encryption becomes. Internet marketing has had a large impact on several industries including music, banking and flea markets – not to mention the advertising industry itself. In the music industry, many consumers have begun buying and downloading MP3s over the Internet instead of simply buying CDs. The debate over the legality of duplicating MP3s has become a major concern for those in the music industry. Internet market has also affected the banking industry. More and More banks are offering the ability to perform banking tasks online. Online banking is believed to appeal to customers because it is more convenient than visiting bank branches. Currently, over 50 million U.S. adults now bank online. Online banking is now the fastest-growing Internet activity. The increasing speed of internet connections is the main reason for the fast-growth. Of those individuals who use the Internet, 44% now perform banking activities over the Internet.

In November, 2004 a lawsuit was filed against Bonzi Buddy software. The lawsuit alleged that Bonzi's banner ads were deceptive. These ads often looked like Microsoft Windows message boxes. Internet users would run across the ads and when they attempted to close the boxes, they found themselves redirected to a website determined by Bonzi. On May 27, 2005, Bonzi Buddy agreed to change the format of its ads so they did not resemble Windows message boxes. The boxes will now contain the word "Advertisement" so computer users know what they are looking at. The boxes will also no longer carry buttons that do not perform the correct actions.

Sales tax issues have also recently become the debated. In the USA, the current laws require that buyers of online products pay their state all due taxes on these goods at the end of the year, along with their other state taxes. However, most consumers do not appear to be making these payments. Thirteen states have now begun encouraging Internet Businesses to collect Sales Tax on every sale. These states are currently not forcing the companies to collect the tax. However, it appears that if companies do not begin collecting the sales tax on their own, states will begin forcing the companies to do so. The states are claiming that each year they lose $ 15 billion in unpaid sales taxes associated with online purchases. However, in Indian context introduction of GST has made positive way for enhancing the tax revenue of Government including from online sale. Whether we like it or not security and digital or cyber security in specific can't be afterthoughts and can't be addressed with just traditional ad hoc and limited point solutions. Cyber security has become a key strategic priority for digital business and is a topic (along with compliance and data usage) we need to be open about if we want to succeed in digital transformation. Moreover, in order to be able to innovate and realize their digital potential in regards to any given business and customer goal, organizations want security approaches that enable them to focus on their business, a phenomenon which is changing the face of the cyber security industry.

ROLE OF CYBER SECURITY

With digital connectivity, the risks of cyber-crimes increase. With multitudes of people using e-commerce and transacting online, there is a huge need for technologies that can prevent data theft. India features in the top 10 secure countries for DDoS attacks – an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. There has been a significant increase in the Internet scams and hacks, with IoT devices being most vulnerable, as they are the major sources of data. The RBI is directing banks to deploy cyber security policies and cyber crisis management plans. Going forward, these policies will get more stringent and prescriptive with broader issues in cyber security being covered under its ambit.

India is also collaborating with the US to develop a complete framework on the India-US cyber relationship. The spending on cloud-based security solutions will continue to increase across verticals, leaders here being the BFSI and online retail companies. The Government too has set in motion a number of initiatives that will take effect in the coming years. Among these the focus is on protecting national crucial information and infrastructure. This would aim to protect key installations and systems across different verticals. Corporate such as Microsoft and Akamai are also establishing specialized centres to develop machine-learning based detection technologies. Specialised teams trained in mitigation of a variety of attacks are also being actively deployed by these technology giants in India. We need more such initiatives to be able to tackle cyber threats in the country. What it

boils down to is indigenous talent and resources with the right skill-sets execute such projects. India is witnessing a huge demand for such security professionals (technologists and analysts, alike). In line with these growing demands, security has become one of the key focus areas for NASSCOM's sector skill council, which working towards creating the right cyber security skill sets among IT professionals.

The Government will need to continue to build momentum in creating new policies to drive Internet adoption and to support the growth of Internet businesses. Whether around broadband spectrum, Internet adoption/availability, data protection, or cyber security, what was applicable five years back is more relevant in today's context, and new policies will need to be futuristic. They will also need to be cognizant of India's challenges and figure out ways to mitigate those challenges. The goal, then, is to create a sustainable environment of public-private partnerships where the ultimate beneficiaries are the citizens of India.

The user experience matters. Performance and agility matters. And, yes, security matters, as long as it doesn't influence these other factors. It's probably the reason why we should think security first as well in our transformation and digitalization efforts and why security is a bit becoming built-in everywhere from the holistic vendor perspective.

Still, many organizations keep steering away too much from the issue of security and avoid being confronted with it, despite saying it's crucial. A mentality shift is needed. In the digital transformation reality the focus is a lot on speed, optimization, automation, innovation and all those other-intermediary-goals. But it should also be on security (and of course compliance). If we want to reap the full benefits of transformation, innovation and digitalization, we also need to take that crucial security part into account because without it we forget the fundamentals, now more than ever. Security is a must in the present and we need to stop looking at security as a cost centre or from an archaic perspective.

SECURITY AND RISK MANAGEMENT IN INTERNET MARKETING

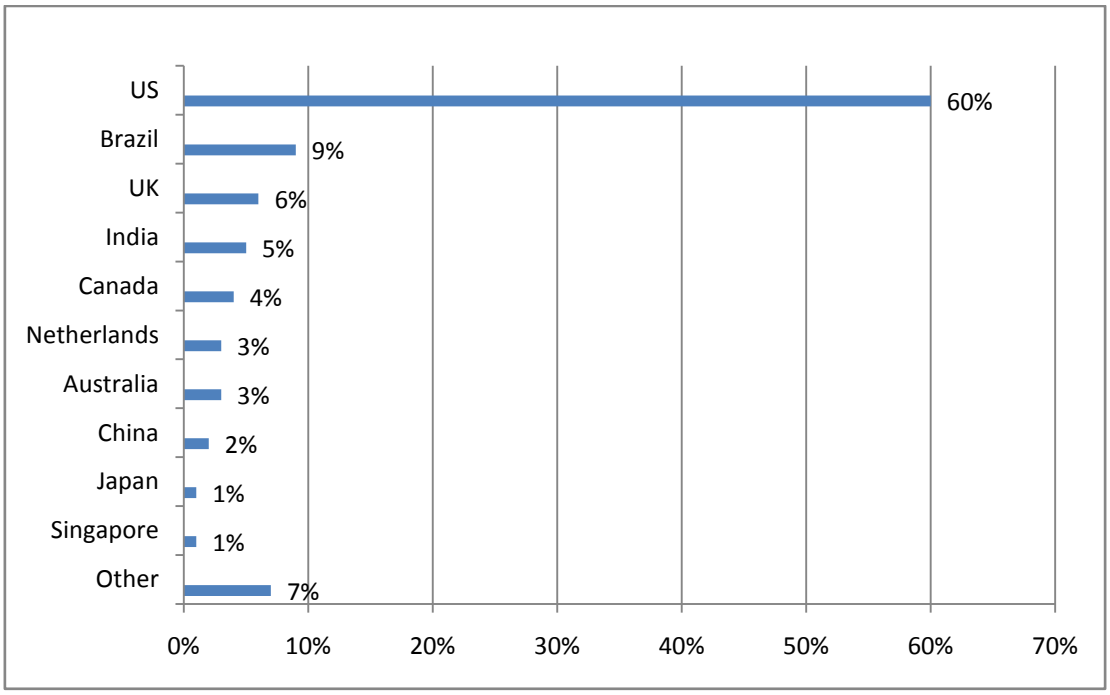
Widespread diffusion of the Internet in India will be contingent on trust in the medium, which in turn is dependent on provisions and perceptions of security of the medium. As with other parts of Asia, mobile data traffic is projected to witness spectacular growth, and could reach 1.7 Exabyte's per month by 2020.

Content access and transactions will be defined by the processes, systems and technologies for security. Unfortunately, the size, frequency and vectors of threats are increasing globally. There are a growing number of web applications and DDoS (Distributed denial of service) attacks. It has become easier for attackers to launch or

participate in an attack, and knowledge of application vulnerabilities is spreading. The number and availability of attack tools are proliferating and DDos-based extortion is on the rise in the BSFI sector.

Attack tools have continued to grow more sophisticated and many attack patterns are being replicated by copycat entities, according to Akamai's State of the Internet Report, Q1 2016. The most common attack vectors include, CHARGEN, DNS, HTP GET, ICMP, NTP, SSDP and SYN Floods; target sectors are business services, education, financial services, gaming, hotel and media. India unfortunately figures in the list of Top 10 source countries and Top 5 target countries for web application attacks in Q1 2016.

Fig: 1.1
Top 10 Target Countries for Web Application Attacks, Q1 2016



Source: www.alkamai.com

India data from CERT-In also indicates a threat increase from 2013 to May 2016. Legislation around cyber security had been and open to interpretation, leading to check in the box solutions across the board. Attack types include not just website defacement but more sophisticated attacks.

Fig. 1.2: Defacement Attacks on Indian Websites

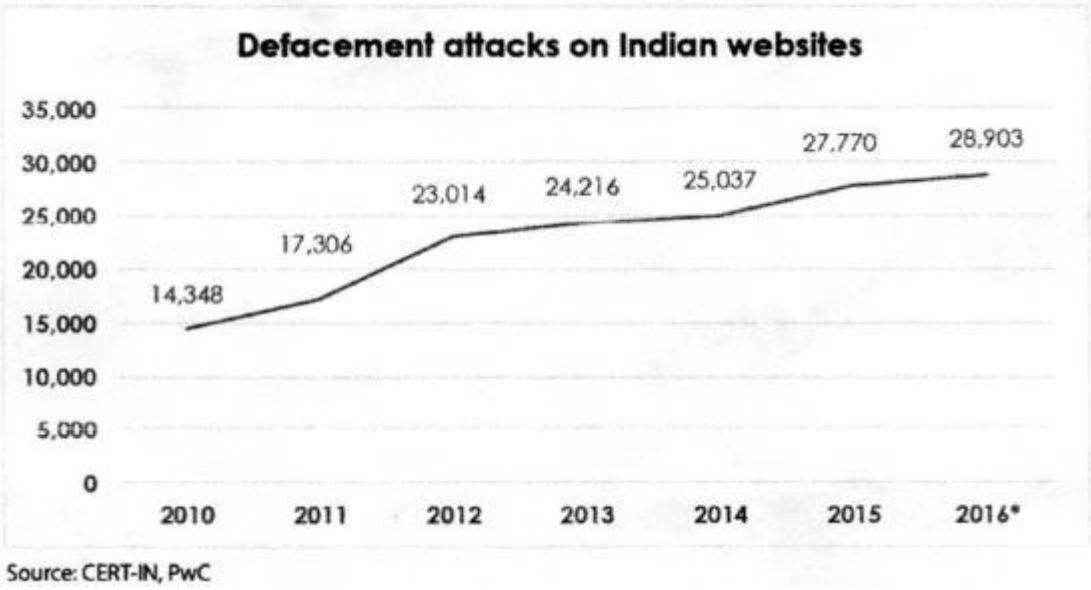
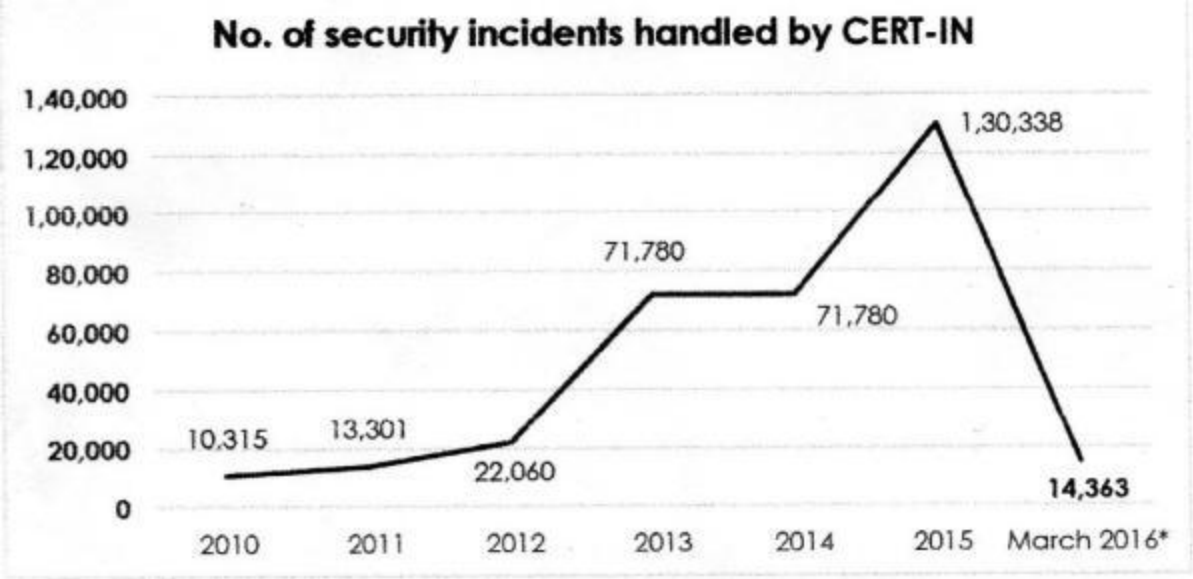


Fig: 1.3



Source: CERT-IN, PwC

These forms of attack include cybercrime, political hacktivism, espionage and cyber terrorism.

The attacks are actioned with the following vectors:

- Application, endpoint, infrastructure threats
- DDoS threats targeting the network and application layers
- Application layer threats that cause data theft

- Direct to origin threats, that are easy to execute have been common occurrence in India

These forms of attack incur serious financial losses to companies and the economy, in terms of loss of revenue, consumer information, and damage to identity and brand. Some of these losses are directly quantifiable, others have broader qualitative impacts.

GOVERNMENT INITIATIVES TO HASTEN INTERNET SECURITY

A number of government departments are involved in the process of hastening internet security, and cooperation between them helps align and harmonies the legislation. These include Department of Electronics and Information Technology (DeitY), National Critical Information Infrastructure Protection Centre (NCIIPC), CERT-In, the Telecom Regulatory Authority of India (TRAI), Education and Research Framework (ERNET), National Informatics Centre (NIC) and the Data Security Council of India (DSCI). DeitY has released notification on the National Cyber Security Policy, and preparing policy papers on cybercrime and the International law framework, including recommendations on what the Indian approach could be. DeitY is also directly responsible for institutes like UIDAI and National Internet Exchange of India.

NCIIPC tracks and alerts government agencies (e.g. banks, railways, power, defence) about potential cyber-attacks. Indian Computer Emergency Response Team (CERT-In) (Under the Ministry of Electronics and Information Technology) addresses a range of cyber security threats to infrastructure and coordinates cyber incident response activities.

ERNET's security activities include providing government securities with the latest antivirus signature. NIC's offices in each state of India provide anti-virus support and security services at state and district levels on a regular basis. The Data Security Council of India (DSCI), set up by NASSCOM, helps best practices and frameworks on security, and publishes studies and papers on the topic.

CONCLUSION

The Internet offered the tremendous potential of exploring countless niches that were simply unsustainable in the offline. But there are many stumbling blocks in the growth of this new form of electronics marketing. The biggest stumbling block for the flattering of Internet vendors is the idealistic approach to the net. Thinking too big and assuming that a huge market is instantly accessible are common misconceptions. A second reason is the improper assessment of consumer behaviour. Added to this, there are many problems-faced by the customer and

the concerned company- relating to e-marketing. These have to be resolved. First, we have to identify these problems.

Digital transformation is about change, agility, speed, connectivity, real-time economy, customer expectations, disruption and all those "hot" things we just mentioned. Security in the eyes of many stands in the way of all this. In a recent survey, more than 3 in 4 (76 per cent) of respondents believe security is brought in too late to digital transformation initiatives. So, security is about rules and regulations, protection, defense (even if in reality cyber security become pro-active and offense), training, awareness, boring stuff (to some) and a layer that some believe to slow down the sexy digital transformation initiatives. Marketing wants a new way to transform how it markets and serves customers or optimizes customer experience; it doesn't want security to poke in there. Well, that too unfortunately is not really an accurate view anymore. Security experts and performance affected by security solutions. Guess what: it doesn't have to (anymore) and can even be done in the cloud. Still, security tends to get called in quite late in digital transformation projects. That's also what research by Dell and Dimensional Research found. According to the Research, a majority of respondents feels that the security team gets involved in digital transformation efforts cloud be blocked reasons excess are scared that their digital transformation efforts cloud be blocked by (the intervention of) security. The doesn't seem like a valid excuse to us, at least not with today's security solutions and certainly not by pretending security isn't crucial. Security isn't always easy and doesn't start by adding security controls but by prioritizing the most crucial processes, systems and potential sources of attacks or vulnerabilities. Needless to say that in the realm of the Internet of Things, vulnerability risks increase by the way. So, security needs a strategy and that is harder than adding a few firewalls of course. Mobility, growing connectivity of technologies, people and processes, and the expansion of networks and clouds to include over more data, devices and decentralized ways of working, have made the new security perimeter the everything. It ranges from traditional perimeters that still exist to the user as a perimeter and even the Internet as a perimeter. That's an enormous difference with how cyber security was viewed upon only a few years ago.

The solution to address all these new cyber security risks and realities, which is not just a choice in this age of digital transformation and ubiquitous connectivity, as said, is by definition a holistic one that includes all the mentioned elements. But it's also one that approaches security in different and more encompassing ways.

Most organizations are aware of this but as we saw there is a gap between realizing cyber security is now a key priority, moving into the bedroom, and needs far more attention and the ability to do so as there is an overall digital crime gap, including between the number and type of attacks organizations face and how they can react.

REFERENCES:

1. Sumanjeet (2006), E-marketing: Strategy Issue, Journal of Marketing and Communication, Vol. 2, No.2, September-December, p. 37

3. www.wikipedia.com

5. www.rbi.org

6. The Future of Internet in India, NASSCOM, Noida, 2016, pp. 48-49

7. Report on Study on Cost of Cyber Crime conducted by Ponemon Institute in the year 2016.

8. Website of Union Bank of India

9. FICCI – KPMG India Media and Entertainment Industry Report 2015.

10. www.ndtv.com

11. Website of Department of Electronics and Information Technology (DeitY), Government of India

12. Website of The National Critical Information Infrastructure Protection Centre

13. Website of The Data Security Council of India

14. Consultation Paper on Issues Related to Digital Terristorial Broadcasting in India, Consultation Paper No. 8/201, The Telecom Regulatory Authority of India, June 2016.