ABSTRACT: The reverberations of the Digital era has transformed the economy in unimaginable ways. Extraordinary developments are being witnessed with changing times. There has been a remarkable growth in network externalities as it tends to the requirement of its multi users. With the advancement of digitized environment, the routine transactions are being effected without employing cash regularly. This perhaps can be subjected to individual notion about preferences and its validity depends upon its employment. In view of such occurrence, the safety of the ongoing transactions has become a matter of utmost concern. Cyber security is being termed as the need of the hour with the growing E-transactions and E-commerce. The entire realm of safeguarding the assets is based on the infrastructure and capacity of the deployed measures to keep the services in place. This paper will highlight the outcome of different security methods employed in the implementation of web based business along with its authenticity.

Keywords- Information Technology, I.T., E Commerce Security, Digitization, Cashless economy.

1. Introduction

The word cashless in itself is an inclusion of various implications. This has augmented the demand for digitization and usage of technicalities to meet the expectations in making routine transactions possible. The heightened growth of the World Wide Web along with the measures that facilitate in its cost effectiveness has assisted in multi dimensional approach. The trade and commerce which were earlier in oblivion of the adoption of I.T. proficiencies, now witnessed a transformed picture of its repercussions and efficiencies. Traditional commerce has now been overpowered by the tremendous acceptance of IT practices giving way to Electronic Commerce. Reduced cost accompanied by better relationship and variety offered in transacting are few advantages of using electronic commerce.

The rapid advancement of technology in the late 90s established a sense of euphoria amongst its users of electronic commerce, eventually leading to the famous burst of the Dot Com Bubble and giving a sense of fluctuating outcomes in the field of Information Technology.(Dotcom Bubble)\(^1\). In the early 2000s, the e-commerce once again regained its dominance and accounted for increase in
retail sales in the United States to approximately 14% over traditional trading mechanisms. (Williams, Hernandez, Petrosky, & Page, 2009)

The major commerce is now a part of electronic commerce. The security and privacy of the aforementioned development has now become a matter of utmost concern. The data along with the basic payment facilities provided by the computer system in effecting everyday transactions are exposed to various kinds of threats and risks. The mobile commerce is being used by 1.6 billion people globally; this figure is witnessing a growth and may increase to two billion mobile phones users by the beginning of 2018. The retail sales in the United States will be accounting for 27% by mobile commerce towards the end of 2018. (Shukairy, 2017)

With such share of sales served by the online medium, the risk involved can be easily deciphered. Cashless mediums, perhaps, are at a risk which needs to be addressed in real time.

II. Objectives Of The Study

1) To understand E-commerce and its basics.
2) To study an outline of trust and security in E-commerce.
3) To understand security measures for E-commerce.

III. E-Commerce Basics

Electronic Commerce being a part of electronic business accounts for major issues encountered in effecting a transaction. The online medium employed by customers in arriving at better deals involves trust and security. The exposure of intimate details on a web to the third party is subjected to greater menace and keeps safety at stake. E-commerce engages customers online for making business transactions by taking into consideration the use of market space rather than marketplace. If not for the internet, the existence of E-Commerce may not be probable. Internet acts as a catalyst for the e-commerce in providing better quality products at a reasonable price and appropriate delivery incentives.

Internet comprises of networks consisting of thousand of networks, being public as well as private and thus being interconnected with each other. Public network is subjected to diversified danger whereas a private network is exposed to threats from the public network itself. On a global platform, documents and data are even more prone on getting attacked by the viruses and other threats prevailing over the web. According to the survey made by security scans on 60,000.00 Magento websites, it was revealed that around 78% of the ecommerce sites are at risk. (Jackson, 2017). The companies like Oracle, Yahoo etc. are likely to face the aforesaid hazard. Active intelligence team carried out by the Cyber security companies is tracking and analyzing the moves of such menace in order to provide a strong background of e-commerce websites. Developers trying to create and maintain a web site are often informed about the intricate details of the firms and thus pose a higher threat due to the assumed knowledge possessed by them.

Five Global Risks while doing E Commerce as follows (Mazars, 2017)

1) Increase in Competition
2) Efficiency and Effectiveness
3) Business model
4) Digital Reputation
5) Cyber Security: Privacy issues of data and information.

The Global E Commerce Survey, 2017 states in its report that 66% of global consumers plan on purchase of mobile in near future. In addition to the aforementioned reporting, consumers cite ‘trust’ as the major barrier in making their purchase online. On the other hand, one in five of the world’s population has done online shopping within a span of one month. (RSA, 2017)
IV. Achieving Trust And Security In An E Commerce Environment

1. Trust

Traditional commerce signifies the presence of a physical vendor whose authenticity can be verified. Personal touch in performing transactions, a sense of security helps in establishing trust between both the parties. This essence of direct contact and personal verification is missing while doing e-commerce and therefore it constitutes in lack of trust and viability.

There are certain levels of trust that has to be achieved while doing E Commerce transactions (Gustavsson & Johansson, 2006)

Information Phase: This phase is the initial platform in building the trust in customers
Agreement Phase : This phase facilitates in making the initial trust a bit stronger, i.e. confirming trust
Settlement Phase : This phase eventually maintains the trust which was acquired in first and second stage.

Even the trust is affected due to the presence of characteristics and issues. The major factors influencing trust in e-commerce are as follows (Suresh, 2015)
(a) Presence of trust marks to reassure customers, (b) A colleague or friend recommending a website, (c) The site displays contact number and address details, (d) Presence of return policy along with reviews.

2. Security

The security threat ranges from high to low relating to convenience and aspect of certain digital requirement. Customers themselves have a perception about the details that they consider highly secure rather than others. For instance, purchasing from a seller directly without logging in to e-commerce websites/company provides a sense of larger risk. This is due to the fact that the
authentication and integrity is more visible at websites medium. Chances of repudiation are also a lot lower. In view of the above revelation, the banking related transactions are considered as secured as compared to the usage of social media and gaming transactions.

![Consumer Security](image)

**Figure 2 : Consumer Cyber Security Confidence Index (RSA, 2017)**

The feeling of security is subjective in its approach. The fact that a large amount of sensitive data pertaining to innumerable customers is available online makes it all the more delicate and tricky. The information that is freely available on the web is also viewed as unauthentic and dicey. Lack of personal touch and trust makes it difficult for the consumers to strike a comfortable deal over the internet.

Presence of certain requisites in deriving proper e-commerce was highlighted while doing this research. They are as follows: a) authentication, b) confidentiality, c) data integrity, d) privacy concern and e), non repudiation. (Maniam, Naranjo, & Subramaniam, 2012)

Unaware customers are the ones who face breach of trust due to security failures. Technical efficacies are misunderstood by customers and they are unable to perform the required work which eventually leads to hacks and breach.

**V. Threats To E Commerce Environment**

The risks and threats involved may arise due to unfair means, stealing of data, fraud and misrepresentation. Accidental threats may happen once in a while and can be recognised and removed but the act to deceive is camouflaged in numerous ways. (TechGen, 2017)

The threats can be as follows:

a) Manipulation of Prices is a much observed phenomenon making it as an act of deception. The prices are sometimes altered in the process of reaching the payment gateway thus charging high prices from the customers.

b) Malicious codes mainly involve
   - Trojan horse: a code which performs destructive functions
   - Viruses: External programs designed to perform its unwanted event
   - Worms: It slows down a computer system by using up its bandwidth and memory.

c) Hacking activism

d) Unsecured Wi-Fi threats
e) Phishing may also account as threat as it refers to the act of obtaining confidential and private information by the third party  
f) Occurrence of data breach in an organization, perhaps can lead to data threat  
g) Credit card frauds  
i) Threats regarding stealing of data and Intellectual property (without owner’s permission)  
j) Server threats including file transfer and spamming

VI. Building Trust And Providing A Secured Environment.

There are types of data that the consumers are more concerned about than the others. The social life that they want to display have another level of issue, however details like their account number, card number are subject to higher risk and therefore require authenticity from the E vendor. On the contrary, details regarding their health and insurance records are not much of apprehension, as only one fifth of the population cites wellness information as confidential. This can be mentioned that consumers have gradually changed over time in consideration to their preferences. (RSA, 2017)

![Figure 3: Varying sense of security from Consumer Cyber Security Confidence Index (RSA, 2017)](image)

The trust can be established by providing customers the required details about the third party and vendors. The customers must be made aware of the technological advances and high personified software. The E vendor must impart all the knowledge about the products and services that he is going to deliver. Trust is directly proportional to the knowledge that we acquire within a course of time.

VII. Implementing Proper Security Measures

For Customers

1. Secured purchases – Customers must check domain names and URL while performing transactions or purchasing something online. Phishing websites may procure and use the data obtained. However, there are other hacks to check the security of a website. A secured website uses encryption to perform any transaction and involves a key without which unlocking the code would be unlikely. It is considered as more secure than telephone and thus provide a reassurance in effective the appropriate process. The confidential information can be transmitted by using technologies like Secure Sockets Layer.  
The Software of the E vendor operating the website must be of an updated version in accordance with the developer so as to remove any unwanted restrictions.  
The websites often displays a lock sign signifying the secured and non secured version, thus this should also be taken into consideration.
2. Security and Privacy Policy should be verified by the customers. – Every website doing e-commerce constitutes a separate privacy policy; the customer must examine all the crucial details attached with its Privacy statements. Sometimes, the vendor may share details with the third party and obtain affiliate fee for affiliation or reference.

3. Return Policy and Contact details – The websites which guarantee a policy of return within a limited span of time and provide authentic contact details can be considered secure as compared to site which does not. Address details and a contact number can be used to verify the genuineness before making the purchase.

4. Payment methods – The safest way in making a payment online is to select cash on delivery method. This enables the procurement of the product before making any payment thus verifying the legitimacy of the site and the product. Another method which can be preferred is a credit card method for effecting the payment. The consumers are generally protected by policies by the Government in discharging facilities. On the other hand, debit card generally discloses confidential details to frauds and thieves and is at greater risk.

5. Low prices and great offers in attracting customers. It is always great to find products at low prices but if the prices are way below the reasonable one, it may not be worth enough. The quality may be compromised or you may get fake brands products.

6. Watch out for Cookies- Here the data remains stored in the computer system. Vendor use your data to quickly upgrade your shopping process and eventually use it for every time you shop from the site. This may disclose the details to frauds and imposters and can cause exposure of private data.

For E Commerce Site Owners

1. Storing of Sensitive data – The data of customers are generally in high volume and is considered as sensitive, preferably the payment data that requires privacy and secrecy. Card Verification Value (CVV) and other numbers and accounts are confidential are considered unsafe and subject to risk. E commerce tools mustn’t be relied upon while performing such kind of work. Either data should be stored in minimal quantities or a third party may be contacted for payment solutions and secured transactions. (Messer, 2016)

2. Strong Password Requirement – The requirement for logging in to a site must require for a strong password, so that the details of the customers may not be at risk. Websites that demands a pattern or mandatory requirements are most secure. For instance requirement of upper case, lower case, special character, number in a password may help in securing the data at backend

3. Proper Hosting – The Web space provided should be good for large websites that comprises of large information. A shared hosting may not be very much useful and can bring down the website. Secure HTTPS hosting may be used to get a good rank in the Google and provides better protection (GlobalSign)

4. DDoS Protection – Distributed Denial of Service attacks are getting a frequent phenomenon nowadays, thus these attacks should be reduced and mitigated by deploying appropriate services. Cloud based services offers securiityat a reasonable cost with a high defence mechanism

5. Firewalls – These protect the infrastructure and allow scans on server for ruling out threats and risks. They also help in adapting to the new kind of threats so that the customers may not face
any difficulty in performing transactions. These firewalls may work independently on the server and may have a separate operating system (CIO, 2013).  

6. Backups –Continuous data protection and recovery of the information offsite can be provided through backups. The database consists of details of numerous users and therefore an offsite back up becomes the need of the hour.

VIII. Recommendations And Conclusion

Both, the customers and the E vendors have to take actions to make their while on the internet worthy. Preventive measures must be taken to extract a better outcome of the innumerable details present on the web. Passwords must be changed regularly to preserve important information. Security patches must be applied as and when required. Always have a word with customer care in case of any discrepancy observed.

E commerce is now widely being substituted by M commerce. Customers are installing applications to make their buying and selling easier at a preferable platform. They are imbibing this development in their day to day transactions which all the more brings a requirement for reducing the risks involved in such transactions.

Since, the safety online is at stake, upgradation to a better antivirus software can also help in minimising of constant pressures from the threats over the web.

References

7. RSA. (2017). 2017 CONSUMER CYBER SECURITY CONFIDENCE INDEX. RSA.
10. RSA. (2017). 2017 CONSUMER CYBER SECURITY CONFIDENCE INDEX. RSA.