I J C T A, 9(41) 2016, pp. 805-812 ISSN: 0974-5572

CYBER THREATS AND ITS IMPACT ON E-COMMERCE SITES

Shweta[1], Vikas Deep[2] and Naveen Garg[2]

Abstract: Today, internet has reached in almost every corner of the world and has become a popular medium of communication and to search information. Various organizations and companies are using internet to introduce and promote their products and services, which introduced the concept of E-Commerce. E-Commerce carries out transactions, essentially buying or selling of goods and services by consumers and E-Commerce organizations respectively, over the web. E-commerce provides a cost effective and efficient way of doing business on the web. This paper discusses E-Commerce, cyber threats to E-Commerce sites and impact of these threats on E-Commerce sites.

Key Words: *Ecommerce, Cyber Threats, Hacking. Encryption, Firewalls, Digital Signatures*

I. INTRODUCTION

E-Commerce web sites facilitate ease-of-doing business and also provide platform to spread business to every corner of the world [1]. With the help of E-Commerce, organization can spread their business to national and international markets with minimum investment of capital. An organization can easily reach out more customers, suppliers and best business partners across the globe [2].This huge growth in the popularity of e-commerce has led to a new generation of associated cyber threats [20].

II. CYBER THREATS TO E-COMMERCE SITES

Internet has now become the medium for carrying out the several transactions online. Its 24x7 availability and ease of use made it as the most popular marketing and commercial tool. An e-Commerce website security is a dynamic process where new threats comes-up every day [21]. In today's competitive world e-commerce systems has to retain customers trust, for that a proper planning must be done to keep the system protected against possible security threats. Following five security features must be there in a secure e-commerce application:

- *Authentication*: Authentication establishes proof of identities. It helps in ensuring that the source of an electronic document or message is identified correctly.
- *Integrity*: The integrity of message is lost, when the sender sends the message but its contents are modified before reaching the intended recipient,. Integrity of message must be intact i.e. message must not be manipulated during transition [22].
- *Non repudiation*: It is a situation where the sender denies later on that the message was not sent by him/her. It does not allow the sender of a message to deny the sending of that message.

[1] *Student, Department of Information Technology, Amity University Uttar Pradesh, Noida, India, Email: shweta.yadav800@gmail.com*
[2.] *Asst Professor, Department of Information Technology, Amity University Uttar Pradesh, Noida, India, Email: vikasdeep8@gmail.com, er.gargnaveen@gmail.com*

- *Access control*: Access control determines who has the access of what, because from the security perspective not just everybody can have the access of system [16].
- *Availability*: Availability ensures that the resources are available to authorized persons at all times. [3]

Every electronic system supporting E-Commerce is vulnerable to following abuse and Threats in many ways:

2.1 Fraud:

Direct financial loss is by fraud activities. Financial records might simply be destroyed or funds might be transferred from one account to another, [4]. Not only credit card payments are vulnerable to frauds, Criminals are using malware to manipulate online transactions via computers, phones, and tablets. They steal bank account information to make fraud payments.

2.1.1 Identity theft:

This is the most common type of a fraud that causes concerns among businesses. Here, credit cards are targeted by the fraudsters, as a criminal does not require much to perform a 'card not present' transaction. Traditionally, In identity theft, the fraudsters carry out transactions by using a different identity. They simply forge someone's existing identity instead of coming up with a completely new identity [5]. This is very easy and much faster. Fraudsters use someone's personal data, such as names, email addresses and addresses, as well as account information or credit card, to appropriate someone's identity or commit identity theft. Using these details they order things online by using a fake name and make payments by debiting another person's account or by using someone's credit card information. Usually a stolen password is everything that is required to forge someone's identity. This information is used to command an account, existing with an online store where the data that is required to make payments is already there in the account [23]. Criminal attacks on e-commerce organizations and stealing of customer information come under the category of fraud.

2.1.2 Friendly fraud:

The term is actually a misnomer: Consider a scenario where customer orders goods or services and makes payment for them using a direct debit or credit card. Then, however, he/she knowingly initiates cash back, and claims that his/her credit card or account details were stolen. He/she gets refunded – but keeps the product ordered. This kind of fraud method is usually found with services, such as those in the adult milieus or gambling. Friendly fraud also combined with re-shipping. This is where fraudster, who use stolen payment information to make payment for their purchases uses middleman's address for shipping, who then forwards the goods [24].

2.1.3 Clean fraud:

The idea behind clean fraud is that a credit card data is stolen and is used to make payments, but the transaction is then manipulated to bypass fraud detection mechanism. Much more information collection is needed here than with friendly fraud. In clean fraud, criminals do a sound study of the fraud detection systems, and great details about the rightful owner of stolen credit cards. Then this correct information is then provided during the payment process to bypass fraud detection mechanism. Card testing is usually carried out, before committing clean fraud. The fraudster makes test purchases to check that the stolen credit card information works [25].

2.1.4 Affiliate fraud:

Affiliate fraud is of two types, both of them have the same aim: to pick more money from an affiliate program by manipulating signup or traffic statistics. This is done either by getting real people to log into merchants' sites using fake accounts or by using a fully automated process. This type of fraud is payment-method-neutral, but widely diffused [26].

2.1.5 Triangulation fraud:

The triangulation fraud is committed via three points. The first is a falsified online shop is used to offer highly demanded goods at very low prices. Many a times, additional bait is added, like if the goods are paid for, using a credit card the information then only goods will be shipped immediately. This fake store collects credit card information and shipping address– which is the sole purpose. The second point of the fraud triangle is that the fraudster then orders goods at real store by using stolen name and credit card data, and then ships them to the original customer. The third point of the fraud triangle is, the fraudster uses the stolen credit card details to make further purchases. This fraud generally remains unnoticed for a longer period of time, as the credit card data and order data are now extremely difficult to connect, which results in greater damages [27].

2.1.6 Merchant fraud:.

It's the simplest: The fake online stores offer goods at extremely low prices, but the customer never gets them shipped. The payments are, obviously, kept by this fake online store. This kind of fraud also found in wholesale. It is not exclusive to any payment method, but this is, of course, where no-cash payment methods come into their own.

2.1.7 More international fraud:

The difficulty of keeping international tabs on every single customers, as well as, language barriers pose additional fraud detection and prevention challenges. The major issue in fraud prevention is the absence of integrated system to provide a unified view of their transactions across all market [28].

2.2 The Ph-ear of Phishing :

The term "phishing" was first came into light in the hacking tool AOHell, which contains a function that attempts to steal the financial details and passwords of American Online users [6]. This term derived from the word 'fishing' but is written as 'phishing' which resembles the word ' phreaking ' which is a mechanism of cracking a telephone network. Phishing appeared within a past few years, thus is a relatively recent phenomenon. It has now become an effective tool with cyber criminals [29].
Several characteristics of phishing:

- Criminals get Trojan horses installed on targeted machines to collect details.
- Hackers "generate" login details and distribute them to cyber criminals [30].
- User's computers are compromised to collect information without their knowledge.
- Vulnerable software can't prevent user computers from downloading malicious code.[7]

To make the phishing successful, an attacker uses various methods. Some of the common methods are:

- Link manipulation: In this method of phishing, the attacker inserts a link in an email to some website.
- Graphical Substitution: As the user logon to the phishing website, it manipulates the users screen with the help of Java Scripts that alters the address bar by adding the image of requested URL instead of the attacker's actual URL [31].
- DNS Cache Poisoning: Normal traffic is interrupted by using DNS Cache Poisoning. It makes the Domain Name Server to direct traffic from specified IP address to the fraudster's server IP address [8].
- Filter evasion: In this method of phishing images are used as links instead if text that makes difficult for the phishing filters to detect [32].

2.3 Server Threats:

The server plays the third point of connection in the Client-Internet-Server trio. This trio embodies the E-Commerce path between e-commerce server and user. Servers are vulnerable and these vulnerabilities can be misused by anyone that can cause huge damage or someone can illegally gather information.

2.3.1 Database Threats:

Every E-Commerce system keeps database that store user data and product information is retrieved from this database, which is connected to the web servers. In addition to product information, databases store valuable and knowledgeable data that can cause a huge damage to a business if it is stolen or tampered. Some databases do not provide much security while saving username and passwords. Anybody can get access to the system as an authorized user or can impersonate someone after obtaining user authentication information

2.3.2 Web Server Threats:

Web Server software delivers web pages as a response of HTTP requests. As the complexity of the software increases, the probability of it containing the errors in coding and security loopholes- security issues which provide doors through which hackers or attackers can get entry to the system- also gets higher.

2.3.3 Common Gateway Interface Threat:

A CGI transfers the data from a web server to some other program, like a database. Common Gateway Interface and the program, to which they transfer information, provide active content to the web pages. There is a higher possibility that CGI can pose a security threat if misused, for example, CGI scripts at web servers can be set up to run by setting privileges to unconstrained. CGIs which contains some defects or malicious codes, can provide access to system resources, are capable of halting or damaging the system .These malicious codes or defects then call privileged base system programs that can delete or alter files , or can view confidential user information including usernames and passwords.

2.4 Password Hacking:

Password hacking is the simplest attack against a system based on password, which involves guessing of passwords Guessing of passwords needs access to the three attributes:

- Complement.
- The complementation functions.
- The authentication functions.

If none of these attributes have been changed till the time the guessing of password is done, the hacker can use the password to get access to the system.[9]

2.5 Pharming:

Pharming attacks targets DNS system. This method of attack highly affects the internet routing system by intervening with the lookup process of domain name. Consider an example: customer enters a site name as www. Amazon. in and gets diverted to similar look site without even realizing it[10].

III. E-COMMERCE SECURITY TOOLS

- Public Key Infrastructure.
- Passwords.
- Encryption Software.
- Biometrics: Retinal scan, finger prints, Voice etc.
- Firewalls: Software and Hardware.
- Locks and Bars
- Digital Certificates
- Digital Signatures [11].

IV. IMPACT OF CYBER CRIMES ON E-COMMERCE SITES

Cyber Crime is committed by the fraudsters or deliberate actions of internet users and take advantage of the availability and ease of use of internet. It presents serious integrity threats, quality and safety of most organizational information systems are compromised, and thus the development of effective security mechanisms becomes a priority. Cyber crime involves the use of computer resources to commit illegal or unauthorized acts [12]. Organizations providing online goods and services can get affected seriously, if E-Commerce website is compromised. The significant business implications of a security incident can include, but are not limited to, the following:

- Subsequent loss owing to adverse publicity.
- Criminal charges if that site is found to be in breach of the regulatory requirements or relevant personal data privacy laws.
- Internet fraud is costly and affects brand.
- Market share is lost if customer confidence is impacted.
- Direct financial loss as a result of fraud.

As shown in Figure 1, an average of 5 percent of gross sales (total revenues) was lost due to the Brand and financial impact of internet fraud during the past 12 months. An average of 19 different internet fraud incidents were reported during the same period.[13]

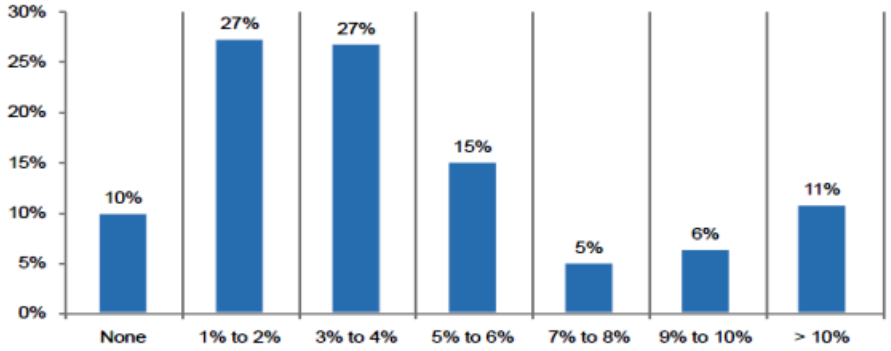

Figure 1: The financial & brand impact of Internet fraud as a percentage of gross sales [17]

4.1 Cyber Attacks Statistics:

- It is clear from the figure 2 that cybercrime activities are spread across the globe. Computer related fraud and forgery is a major concern. [14]

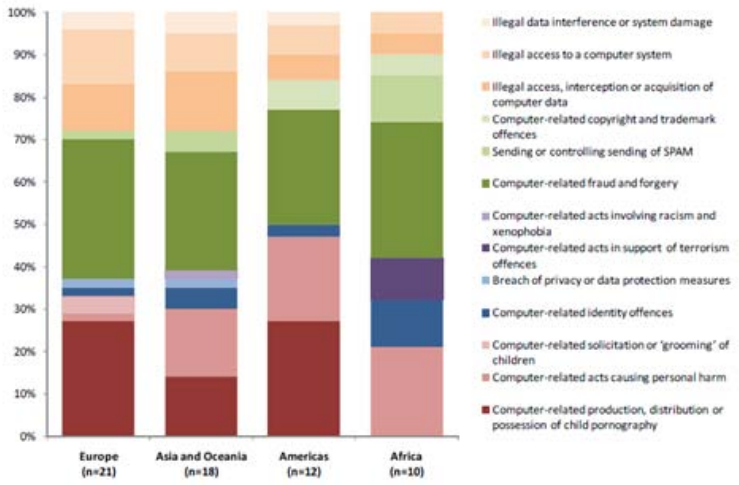

Figure 2: Most common cybercrimes encountered by national police (UNODC) [18]

4.2 Cyber *crime cases in India:*

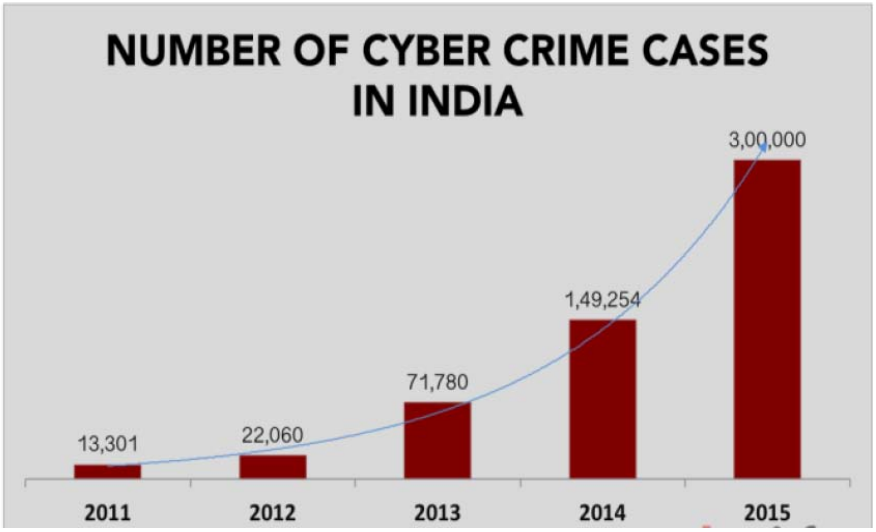

Figure 3: Number of Cyber Crime Cases in India [19]

In the last few years , India has registered 107% 0f common annual growth rate in the number of cyber crime cases registered. As shown in the figure 3, cyber crime cases are growing every year which shows the seriousness of increased misuse of computer resources and internet [15].

V. CONCLUSION

The growth of the internet and various technologies has made E-Commerce functions to get executed fast and easier. Very huge amount of transactions are being performed these days through ecommerce and a large amount of data is being stored. So, E- Commerce security is a major concern and better security can be provided only if we know about the threats and frauds better.

REFERENCES

[1] Arti, Sunita Choudhary, and G. N. Purohit. "Role of Web Mining in E-Commerce.".

[2] Kidane, Teklehaimanot Tadele, and R. R. K. Sharma. "Influence of culture on E-commerce and vice versa."

[3] Udo, Godwin J. "Privacy and security concerns as major barriers for e-commerce: a survey study." Information Management & Computer Security 9.4 (2001): 165-174.

[4] KOHLI, GAUTAM. "E-COMMERCE: TRANSACTION SECURITY ISSUE AND CHALLENGES." CLEAR International Journal of Research in Commerce & Management 7.2 (2016).

[5] Maurya, Santosh Kumar, and NagendraPratap Bharati. "Cyber Security; Issue and Challenges in E-Commerce." PARIPEX-Indian Journal of Research 5.1 (2016).

[6] Jarnail Singh- 'Review of E-Commerce Security Challenges'. International Journal of innovative Research in Computer and Communication Engineering, 2014.

[7] Mathew, Alex Roney, Aayad Al Hajj, and Khalil Al Ruqeishi. "Cyber crimes: Threats and protection." 2010 International Conference on Networking and Information Technology. IEEE, 2010.

[8] McCrohan, Kevin F. "Facing the threats to electronic commerce." Journal of Business & Industrial Marketing 18.2 (2003): 133-145.

[9] Lokhande, Prashant S. "E-Commerce Applications: Vulnerabilities, Attacks and Countermeasures." (2013).

[10] Niranjanamurthy, M., and DR Dharmendra Chahar. "The study of e-commerce security issues and solutions." International Journal of Advanced Research in Computer and Communication Engineering 2.7 (2013).

[11] Leena, N. "Cyber Crime Effecting E-commerce Technology." Oriental Journal of Computer Science & Technology 4.1 (2011).

[12] Statistics, Cyber Attacks. "Hackmageddon." Avaialble online: http://hackmageddon. com/category/security/cyberattacks-statistics (2015).

[13] Cashell, Brian, et al. "The economic impact of cyber-attacks." Congressional Research Service Documents, CRS RL32331 (Washington DC) (2004).

[14] Ghosh, Anup K. E-commerce security: weak links, best defenses. Wiley, 1998.

[15] Lallmahamood, Muniruddeen. "An Examination of Individual's Perceived Security and Privacy of the Internet in Malaysia and the Influence of this on their Intention to Use E-commerce: Using an Extension of the Technology Acceptance Model." Journal of Internet Banking and Commerce 12.3 (2007)

[16] Kim, Dan J., Charles Steinfield, and Ying-Ju Lai. "Revisiting the role of web assurance seals in business-to-consumer electronic commerce." Decision Support Systems 44.4 (2008): 1000-1015.

[17] https://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf

[18] http://resources.infosecinstitute.com/2013-impact-cybercrime/#gref

[19] http://gendermatters.in/2016/05/cyber-crime-laws/

[20] Chhikara, Pallavi, Gurpreet Singh Matharu, and Vikas Deep. "Towards OpenFlow based software defined networks." Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on. IEEE, 2014.

[21] Aggarwal, Sahil Kumar, Vikas Deep, and Robin Singh. "Speculation of CMMI in agile methodology." Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on. IEEE, 2014.

[22] Singh, Pravinder, Monica Lamba, and Vikas Deep. "A Survey on Zone Routing Protocol Techniques." International Journal of Innovations in Engineering and Technology (IJIET) Vol 2 (2013).

[23] ur Rahman, Munib, et al. "Implementation of ICT and Wireless Sensor Networks for Earthquake Alert and Disaster Management in Earthquake Prone Areas." Procedia Computer Science 85 (2016): 92-99.

[24] Tanwar, Rajneesh, et al. "Railway Reservation Verification by Aadhar Card." Procedia Computer Science 85 (2016): 970-975.

[25] Lal, Divya, et al. "Advanced Immediate Crime Reporting to Police in India." Procedia Computer Science 85 (2016): 543-549.

[26] ur Rahman, Munib, Vikas Deep, and Santosh Multhalli. "Centralized vulnerability database for organization specific automated vulnerabilities discovery and supervision." Research Advances in Integrated Navigation Systems (RAINS), International Conference on. IEEE, 2016.

[27] ur Rahman, Munib, Vikas Deep, and Soliha Rahman. "ICT and internet of things for creating smart learning environment for students at education institutes in India." Cloud System and Big Data Engineering (Confluence), 2016 6th International Conference. IEEE, 2016.

[28] Chaudhary, Lalita, et al. "Business Modeling Using Agile." Information Systems Design and Intelligent Applications: Proceedings of Third International Conference INDIA 2016. Vol. 1. Springer, 2016.

[29] Chaudhary, Lalita, Vikas Deep, and Preeti Chawla. "Systematic Evaluation of Seed Germination Models: A Comparative Analysis." Information Systems Design and Intelligent Applications. Springer India, 2016. 59-65.

[30] Jain, Renu, and Vikas Deep. "Expert system for the management of insect-pests in pulse crops." Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on. IEEE, 2015.

[31] Chawla, Preeti, et al. "Systematic overview of mobile virtualization platforms: Comparative analysis." Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on. IEEE, 2015.

[32] Sharma, Anshul Kumar, Vikas Deep, and Naveen Garg. "An efficient way of articulation or suppression in agile methodologies." Confluence 2013: The Next Generation Information Technology Summit (4th International Conference). IET, 2013.